EVALUASI KEAMANAN SISTEM INFORMASI RSUD ARIFIN ACHMAD PEKANBARU MENGGUNAKAN ISO 27001

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

MOHAMAT IQBAL
11553102542

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2021

LEMBAR PERSETUJUAN

EVALUASI KEAMANAN SISTEM INFORMASI RSUD ARIFIN ACHMAD PEKANBARU MENGGUNAKAN ISO 27001

TUGAS AKHIR

Oleh:

MOHAMAT IQBAL
11553102542

Telah diperiksa dan disetujui sebagai laporan tugas akhir
di Pekanbaru, pada tanggal 21 Juli 2021

Ketua Program Studi	Pembimbing
Idria Maita, S.Kom., M.Sc.	**Eki Saputra, S.Kom., M.Kom.**
NIP. 197905132007102005	**NIK. 198307162011011008**

LEMBAR PENGESAHAN

EVALUASI KEAMANAN SISTEM INFORMASI RSUD ARIFIN ACHMAD PEKANBARU MENGGUNAKAN ISO 27001

TUGAS AKHIR

Oleh:

MOHAMAT IQBAL
11553102542

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 05 Juli 2021

Pekanbaru, 21 Juli 2021
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Hartono, M.Pd.	Idria Maita, S.Kom., M.Sc.
NIP. 196312141988031002	NIP. 197905132007102005

DEWAN PENGUJI:

Ketua : Idria Maita, S.Kom., M.Sc.

Sekretaris : Eki Saputra, S.Kom., M.Kom.

Penguji 1 : Syaifullah, S.E., M.Sc.

Penguji 2 : Inggih Permana, S.T., M.Kom.

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin penulis dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi,Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 05 Juli 2021

Yang membuat pernyataan,

MOHAMAT IQBAL

NIM. 11553102542

LEMBAR PERSEMBAHAN

Alhamdulilah dengan mengucapkan syukur saya lantunkan kepada Allah SWT, karena sudah memperkenalkan saya kepada orang-orang yang sangat berarti disekeliling saya. Yang selalu memberi semangat dan doa yang tak hentinya, sehingga Tugas Akhir saya ini dapat diselesaikan dengan baik. Apa yang saya dapatkan hari ini, belum mampu membayar semua kebaikan dari orang-orang yang berada disekeliling saya. Dan saya persembahkan Tugas Akhir ini sebagai wujud terima kasih untuk:

1. Ayahanda tercinta, bapak Yohanson yang telah merawat saya, selalu memberikan dorongan dan motifasi kepada saya, selalu memenuhi kebutuhan yang saya minta sampai sekarang ini, selalu memberikankan waktunya dan tenaganya dan yang terus memberikan kasih dan sayang yang tak terhingga.
2. Ibunda tersayang, ibu Yuni Rika yang telah mempertaruhkan nyawanya agar saya terlahir didunia ini, selalu memberikan waktu dan tenaganya untuk merawat dan membesarkan saya, tanpa rasa lelah hingga hingga saat sekarang ini, dan yang selalu memanjatkan doa disetiap sujudnya untuk anak-anaknya, tanpamu saya bukanlah siapa-siapa.
3. Ria Utami kakak kandung yang saya sayangi, yang selalu menjadi panutan dan kebanggaan keluarga serta menjadi seorang yang sangat menyayangi orang tua dan adiknya.

Demikian lah ucapan persembahan dalam penulisan Tugas Akhir saya, dan saya ucapkan beribu terimakasih kepada orang-orang yang sangat berarti bagi saya. dan semoga kita semua diberikan kesehatan dan keberkahan, Aamiin.

”Ilmu tanpa agama adalah sesat,Agama tanpa ilmu adalah buta”

-MOHAMAT IQBAL-

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Allhamdulillah hirobbil'alamiin. puji beserta syukur kita lantunkan atas kehadirat Allah SWT yang sudah memberikan berkah beserta hidayah-Nya kepada kita, sehingga penulisan laporan Tugas Akhir ini dapat berjalan semestinya dan akhirnya dapat diselesaikan. Shalawat ber iring salam kita haturkan kepada junjungan kita yaitu Nabi Muhammad SAW yang menjadi uswatun hasanah, suri tauladan yang baik kepada kita semua.

Laporan tugas akhir ini adalah salah satu prasyarat untuk memenuhi persyaratan akademik guna mendapatkan gelar S.Kom pada Program Studi Sistem Informasi, UIN SUSKA Riau. Dalam proses penyelesaian laporan tugas akhir ini, penulis selalu mendapatkan bantuan dalam menyelesaikan penulisan laporan Tugas Akhir ini. pada kesempatan kali ini penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Khairunnas Rajab, M.Ag., Rektor UIN SUSKA RIAU.
2. Bapak Dr.Hartono, M.Pd., Dekan Faste.
3. Ibu Idria Maita, S.Kom., M.Sc., Ketua Prodi Sistem Informasi.
4. Ibu Megawati, S.Kom., MT, Pembimbing Akademik ' telah membimbing dan mengasih perhatian dari awal perkuliahan.
5. Ibu Idria Maita, S.Kom.,M.Sc., Ketua Sidang yang sudah mengasih masukan dan saran dalam penulisan Tugas Akhir ini.
6. Bapak Eki Saputra, S.Kom., M.Kom., dosen pembimbing Tugas Akhir saya yang sudah banyak membantu, senantiasa mendengarkan keluh kesah penulis, serta memberikan motivasi kepada penulis dan meluangkan waktu untuk membimbing penulis.
7. Bapak Syaifullah, S.E., M.Sc., Penguji I Tugas Akhir yang sudah memberikan bantuan, mengasih masukan dan arahan demi kelancaran Tugas Akhir ini.
8. Bapak Inggih Permana, S.T., M.Kom., Penguji II Tugas Akhir yang sudah membantu penulis, memberikan masukan dan arahan kepada penulis dalam pennulisan Tugas Akhir ini.
9. Segenap dosen dan pegawai Prodi Sistem Informasi, Faste, UIN SUSKA Riau yang telah memberikan banyak ilmu dan motivasi.
10. Ibuk Ike Emanarni *Administrator* RSUD Arifin Achmad Pekanbaru yang telah memberi izin dan menerima penulis untuk melakukan penelitian.
11. Keluarga penulis yang dicintai, orangtua penulis Bapak Yohanson dan Ibu Yuni Rika yang telah memberikan segalanya, baik itu kasih sayang, seman-

gat, doa dan dukungan yang tak hingga. Semoga Ayah dan Amak dalam lindungan Allah. Amiin Ya Rabbalalamin.

12. Keluarga besar dari penulis, Ria Utami, Fikri Maulana, Muhammad Rheza Fahlevi dan adek-adek sepupu. Terima kasih telah mengasih semangat, perhatian, doa dan dukungannya selama ini.
13. Keluarga Kecil penulis Billy Saputra, Faviansyah Chairi, Dilla Kurniati, Khintan Mayori, Liwaul Hamdi, Hengki Ariandi,Wanda Afita, Raja Huta Hasibuan, Randi Karsono Murti, Jubpri, Fauzul Asmar, Noval Adrian,Khairullah, Mhd. Dhery F, Anggara Sobirin Sholeh, Kissi Amelia Yulia Ningsih dan Syarafina Mardiyah. Terimakasih telah membantu, memberikan dukungan, semangat selama melakukan penelitian Tugas Akhir dan menemani saya sampai terlaksananya sidang, serta memberikan doa yang terbaik.
14. Keluarga SIF E 2015 yang telah membantu dan bersama-sama berjuang melewati kegiatan perkuliahan. Terimakasih atas kebersamaan yang telah kita lewati ini.
15. Teman-teman angkatan 2015 Prodi Sistem Informasi Faste, UIN SUSKA Riau yang sudah berkontribusi.
16. Abang-abang, kakak-kakak, teman-teman dan adik-adik keluarga Program Studi Sistem Informasi yang tidak dapat penulis sebutkan.
17. Serta semua pihak yang memberikan bantuan yang tidak bisa penulis sebutkan.Terima kasih semoga diberkahi dan dilindungi oleh Allah SWT.

maka dari itu penulis sangat berterimakasih kepada semua yang terlibat. dalam penulisan Tugas Akhir jauh dari sempurna, maka sebab itu itu diharapkan masukkan dan kritikan yang sangat berguna demi membangun laporan yang mendekati sempurna dan masukkannya dapat die-mail ke mohamat.iqbal@students.uin-suska.ac.id dan semoga laporan tugas akhir ini bisa berguna untuk semua orang yang membutuhkan.

Wassalamu'alaikum warahmatullahi wabarakatuh.

Pekanbaru, 21 Juli 2021

Penulis,

MOHAMAT IQBAL

NIM. 11553102542

EVALUASI KEAMANAN SISTEM INFORMASI RSUD ARIFIN ACHMAD PEKANBARU MENGGUNAKAN ISO 27001

MOHAMAT IQBAL
NIM: 11553102542

Tanggal Sidang: 05 Juli 2021
Periode Wisuda:

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

RSUD Arifin Achmad adalah salah satu rumah sakit yang telah menggunakan TI sebagai sarana membantu terlaksananya aktifitas di seluruh unit kerja rumah sakit. RSUD Arifin Achmad mempunyai sebuah direktorat yang bernama *Instalasi Electronic Data Processing* (EDP) yang memiliki tugas dalam proses pemeliharaan data dan jaringan seperti, menjaga keamanan data, memberikan hak akses (otoritas), maintenance software yaitu backup data dan *backup system*, bertanggung jawab memastikan seluruh jaringan dan hardware di RSUD Arifin Achmad tidak bermasalah. Berdasarkan wawancara dengan narasumber didapati permasalahan yang berkaitan dengan pengelolaan resiko keamanan informasi diantaranya,tidak adanya kerangka kerja pengelolaan resiko keamanan informasi yang terdokumentasi dan secara resmi digunakan,belum diterapkannya ambang batas tingkat resiko yang dapat diterima,belum diterapkannya secara menyeluruh penanggung jawab manajemen resiko dan eskalasi pelaporan status pengelolaan resiko keamanan informasi sampai ke tingkat pimpinan,serta tidak adanya kajian untuk meningkatkan efektifitas kerangka kerja pengelolaan resiko. untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi. Berdasarkan hasil pengolahan dan pembahasan kuisioner didapatkan dari hasil evaluasi akhir pada tingkat kelengkapan penerapan standar keamanan dengan skor 308 dari skor maksimal yaitu 645 yang berada pada tingkat keamanan “Tidak Layak”.

Kata Kunci: *Electronic Data Processing*,ISO 27001, Keamanan Informasi, RSUD

EVALUATION INFORMATION SYSTEM SECURITY RSUD ARIFIN ACHMAD WITH ISO 27001

MOHAMAT IQBAL
NIM: 11553102542

Date of Final Exam: July 05th 2021
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

Arifin Achmad Hospital is one of the hospitals that has used IT as a means to help carry out activities in all hospital work units. RSUD Arifin Achmad has a directorate called the Electronic Data Processing (EDP) Installation which has duties in the process of maintaining data and networks such as maintaining data security, providing access rights (authorities), software maintenance, namely data backup and system backup, responsible for ensuring all the network and hardware at the Arifin Achmad Hospital are not problematic. Based on interviews with resource persons, it was found that problems related to the management of information security risks include the absence of a documented and officially used work program and framework for managing information security risks, the absence of an acceptable risk level threshold, and the absence of a comprehensive implementation of the person in charge of management. risk and escalation of reporting the status of information security risk management to the leadership level, as well as the absence of studies to improve the effectiveness of the risk management framework. to measure the level of maturity and completeness in information security called the Information Security Index (KAMI). The KAMI index refers to ISO 27001 which contains information security. Based on the results of the processing and discussion of the questionnaire, it was obtained from the results of the final evaluation on the level of completeness of the application of security standards with a score of 308 from the maximum score of 645 which was at the "Not Eligible" security level..

Keywords: *Electronic Data Processing,Hospital,Information Security,Iso 27001*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

CMMI	:	*Capabillity Maturity Model Integration*
COBBIT	:	*Control Objective for Information and related Technology*
EDP	:	*Electronic Data Processing*
HAKI	:	Hak Atas Kekayaan Intelektual
ISO	:	*International Organization for Standaritation*
ISMS	:	*Information Security Management System*
KOMINFO	:	Kementerian Komunikasi dan Informatika
RSUD	:	Rumah Sakit Unit Daerah
SDM	:	Sumber Daya Manusia
SI	:	Sistem Informasi
SIMRS	:	Sistem Informasi Manajemn Rumah Sakit
SMKI	:	Sistem Manajemen Keamanan Informasi
SOP	:	*Standar Operasional Procedure*
TI	:	Teknologi Informasi
TIK	:	Teknologi Informasi Komunikasi
UU	:	Undang-Undang

BAB 1
PENDAHULUAN

1.1 Latar Belakangan

Perkembangan teknologi informasi (TI) setiap hari semakin maju dengan sangat pesat, akibat perkembangan ini seluruh organisasi atau perusahaan harus selalu beradaptasi serta mengimplementasikan kemajuan TI. Didalam teknologi yang perkembangannya semakin pesat tersebut terdapat informasi yang diolah dan disimpan. Informasi merupakan data yang dapat digunakan dalam proses pengambilan keputusan. Untuk menjaga keamanan informasi perlu dilakukan usaha dalam memperhatikan faktor-faktor keamanan dari seluruh piranti pendukung, jaringan, dan fasilitas lain yang terkait secara langsung maupun tidak langsung dalam proses pengolahan informasi.

Keamanan Informasi juga perlu diperhatikan di Rumah Sakit Umum Daerah (RSUD) Arifin Achmad Pekanbaru. RSUD Arifin Achmad adalah salah satu rumah sakit yang telah menggunakan TI sebagai sarana untuk membantu terlaksananya aktifitas di seluruh unit kerja rumah sakit. RSUD Arifin Achmad mempunyai sebuah direktorat yang bernama Instalasi *Electronic Data Processing* (EDP) yang memiliki tugas dalam proses pemeliharaan data dan jaringan seperti, menjaga keamanan data, memberikan hak akses (otoritas), *maintenance software* yaitu backup data dan backup system, bertanggung jawab memastikan seluruh jaringan dan perangkat keras di RSUD Arifin Achmad tidak bermasalah. Pemanfaatan teknologi ini juga sesuai dengan ketentuan Undang-Undang No. 44 Tahun 2009 Tentang Rumah Sakit, yaitu pasal 52 ayat 1: "Setiap Rumah Sakit wajib melakukan pencatatan dan pelaporan tentang semua kegiatan penyelenggaraan Rumah Sakit dalam bentuk Sistem Informasi Manajemen Rumah Sakit".

RSUD Arifin Achmad telah memanfaatkan sistem informasi manajemen (SIMRS) untuk memenuhi peraturan pemerintah seperti yang telah dijelaskan dalam UU No.44 tahun 2009 di atas dan juga untuk menunjang aktivitas bisnisnya. Namun dalam pemanfaatan sistem informasi tersebut, RSUD Arifin Ahmad tidak terlepas dari sejumlah permasalahan baik pada area bisnis, organisasi maupun pengelolaan SI/TI. Adapun system informasi yang sudah terhubung dengan sistem informasi manajemen RSUD Arifin Achmad diantaranya Rekarn medis, instalasi rawat inap, rawat darurat, rawat jalan, farmasi kasier, penjulan obat, bedah sental, radiologi, patologi, rehab medis, bank darah, gizi, akuntansi, keuangan, logistih perbendaharaan, sdm, asuhan keperawatan.

Berdasarkan wawancara dengan narasumber didapati permasalahan yang

berkaitan dengn pengelolaan resiko keamanan informasi diantaranya,tidak adanya program kerja serta kerangka kerja pengelolaan resiko keamanan informasi yang terdokumentasi dan secara resmi digunakan,belum diterapkannya ambang batas tingkat resiko yang dapat diterima,belum diterapkannya secara menyeluruh penanggung jawab manajemen resiko dan eskalasi pelaporan status pengelolaan resiko keamanan informasi sampai ke tingkat pimpinan,tidak teridentifikasinya ancaman dan kelemahan yang terkait dengan asset informasi,serta tidak adanya kajian untuk meningkatkan efektifitas kerangka kerja pengelolaan resiko.

Untuk memperbaiki pengelolaan aset yang ada di Instalasi EDP maka pihak manajemen RSUD Arifin Achmad membutuhkan evaluasi sesuai standar keamanan informasi. Adapun risiko yang bisa ditimbulkan jika pengelolaan aset tidak dilindungi yaitu dari aset informasi ketika data dan dokumen penting mampu diakses dan dilihat langsung oleh orang yang tidak berhak memperoleh informasi yang berharga sehingga mampu memperoleh keuntungan dari pencurian informasiyang dapat menimbulkan kerugian bagi perusahaan. Dari segi aset layanan, risiko dapat berasal dari penyadapan yang dilakukan oleh saluran komunikasi secara tidak sah sehingga mampu memperoleh informasi yang berharga kepada pihak yang bukan wewenangnya. Perlindungan terhadap perangkat keras juga dibutuhkan agar terhindar dari risiko kerusakan fisik yang disebabkan oleh penjahat komputer yang dapat masuk kedalam jaringan komputer yang berada jauh dari lokasi. Perlindungan aset perangkat lunak dilakukan untuk memperkecil risiko modifikasi perangkat lunak yang bisa menyebabkan pengguna yang ada di ouput system menerima informasi yang salah dan membuat keputusan yang salah sehingga dapat merugikan perusahaan. Aset-aset pada Instalasi EDP diidentifikasi risikonya sehingga diharapkan mampu mengurangi risiko yang ada dengan sejumlah kendali keamanan informasi yang ada.

Salah satu upaya yang dapat dilakukan oleh kementrian Kominfo untuk meningkatkan kualitas keamanan informasi pada suatu instansi adalah dengan membuat salah satu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif.

Keamanan teknologi dan sistem informasi merupakan hal yang paling esensial pada RSUD Arifin Achmad. Teknologi dan sistem informasi memiliki peran dalam memajukan perusahaan, namun dapat juga menimbulkan kerugian karena TI

rentan terhdapa ancaman. Sehingga diperlukan kematangan keamanan dan teknologi informasi untuk menjaga data dan informasi perusahaan dengan baik. Untuk mewujudkan hal ini diperlukan kajian yang mendalam terhadap tingkat kematangan dan teknologi informasi di RSUD Arifin Achmad terhadap ancaman. Diharapkan hasil dari evaluasi menggunakan ISO 27001 dapat digunakan RSUD Arifin Achmad sebagai media evaluasi dalam rangka meningkatkan keamanan informasi dari rumah sakit di masa yang akan datang.

Berdasarkan latar belakang tersebut, penulis mengangkat judul **"Evaluasi Keamanan Sistem Informasi RSUD Arifin Achmad Pekanbaru Menggunakan ISO 27001"**

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat diambil sebuah rumusan masalah, "Bagaimana mengevaluasi keamanan sistem informasi RSUD Arifin Achmad Pekanbaru menggunakan ISO 27001?".

1.3 Batasan Masalah

Batasan masalah tugas akhir ini ialah:

1. Penelitian ini hanya mencakup lingkup keamanan informasi pada *Electronic Data Processing* (EDP) di RSUD Arifin Achmad Pekanbaru.
2. Pengukuran dilakukan menggunakan Indeks Keamanan Informasi (KAMI) versi 2.3 yang dikembangkan oleh kementerian Komunikasi dan Informasi Republik Indonesia.
3. Responden merupakan karyawan pada bagian EDP RSUD Arifin Achmad Pekanbaru.

1.4 Tujuan

Tujuan tugas akhir ini ialah:

1. Untuk mengetahui tingkat kelengkapan dan kematangan keamanan informasi pada RSUD Arifin Achmad Pekanbaru khususnya keamanan informasi pada *Instalasi Electronic Data Processing* (EDP).
2. Untuk memberikan rekomendasi perbaikan dalam meningkatkan kelengkapan dan kematangan informasi pada *Electronic Data Processing* (EDP) di RSUD Arifin Achmad Pekanbaru.

1.5 Manfaat

Manfaat tugas akhir ini ialah:

1. Dapat memberikan informasi pengelolaan terhadap keamanan *Electronic Data Processing* (EDP) yang berguna untuk meningkatkan sistem manajeman keamanan informasi pada RSUD Arifin Achmad Pekanbaru.
2. Dapat memberikan rekomendasi perbaikan dalam meningkatkan kelengkapan dan kematangan informasi pada *Electronic Data Processing* (EDP) di RSUD Arifin Achmad Pekanbaru.

1.6 Sistematika Penulisan

Sistematika penulisan laporan Tugas Akhir meliputi:

BAB 1. PENDAHULUAN

BAB 1 pada tugas akhir ini menjelaskan tentang; (1) Latar Belakang; (2) Rumusan Masalah; (4) Batasan Masalah; (5) Tujuan; (6) Manfaat dan (7) Sistematika Penulisan Laporan Tugas Akhir.

BAB 2. LANDASAN TEORI

BAB 2 pada tugas akhir ini berisi tentang: teori-teori yang berasal dari jurnal, buku serta studi kepustakaan yang digunakan sebagai landasan teori dalam pembuatan tugas akhir ini seperti: (1) Keamanan Informasi; (2) ISO 27001; (3) Kerangka Kerja ISO 27001; (4) Indeks Keamanan KAMI; (5) RSUD Arifin Achmad; (6) Penelitian Terdahulu.

BAB 3. METODOLOGI PENELITIAN

BAB 3 pada Tugas Akhir ini berisi tentang: (1) Metodologi Penelitian; (2) Tahap Perencanaan; (3) Tahap Pengumpulan Data; (4) Tahap Pengolahan Data; (5) Hasil dan Dokumentasi.

BAB 4. PEMBAHASAN DAN HASIL

BAB 4 pada Tugas Akhir ini berisi tentang: (1) Evaluasi Keamanan Informasi; (2) Identifikasi Kemungkinan Ancaman Dan Kelemahan; (3) Rancangan Proses Pengukuran Keamanan Informasi; (4) Kerangka Kuisioner; (5) Responden Penelitian; (6) Pembahasan Hasil; (7) Rekomendasi Perbaikan 5 Area Keamanan Informasi.

BAB 5. PENUTUP

BAB 5 pada Tugas Akhir ini berisi tentang: (1) Kesimpulan; (2) Saran.

BAB 2
LANDASAN TEORI

2.1 Keamanan Informasi

Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, memilimalisir risiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (Sarno, 2009). Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara stimultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman, 2011).

1. *Physichal Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi dan bencana alam.
2. *Personal Security* yang overlap dengan *phisycal security* dalam melindungi orang-orang dalam organisasi.
3. *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
4. *Communication Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat untuk mencapai tujuan organisasi.
5. *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya serta kemmpuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen diatas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan dan mengirimkannya. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha.

Menurut (Andress, 2014) terdapat tiga konsep utama dalam keamanan informasi, yaitu kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)*. Kerahasiaan *(confidentiality)* mengacu pada kemampuan untuk melindungi data dari orang-orang yang tidak berwenang untuk melihatnya. Integritas *(integrity)* mengacu pada kemampuan untuk mencegah dari pengubahan pada

pihak yang tidak berwenang dan kemampuan untuk membalikkan perubahan pada pihak berwenang yang perlu dibatalkan. Ketersediaan *(availability)* mengacu pada kemampuan untuk mengakses data ketika data dibutuhkan.

2.1.1 Sistem Manajeman Keamanan Informasi (SMKI)

Sebuah organisasi harus menerapkan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan aset teknologi informasi dan komunikasi (TIK). Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik organisasi secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan (Basyarahil, Astuti, Hidayanto, dkk., 2017)

Sistem Manajeman Keamanan Informasi (SMKI) atau disebut juga dengan Information Security Management System (ISMS) merupakan suatu proses yang disususn berdasarkan pendekatan resiko bisnis untuk merencanakan *(Plan)* mengimplementasikan dan mengoperasikan *(Do)*, memonitor dan meninjau ulang *(Check)* serta memelihara dan meningkatkan atau mengembangkan *(Act)* terhadap keamanan informasi perusahaan. Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan *(Confidentiality)*, keutuhan *(Integrity)*, dan ketersediaan *(Availability)* dari informasi.

Untuk itu SKMI harus didukung oleh hal-hal berikut: perencanaan *(Planning)*, kebijakan keamanan textit(security policy), program *(prosedur dan proses)*, penilaian resiko *(risk assesment)*, sumber daya manusia *(people)* dan tanggung jawab *(responsibility)*.

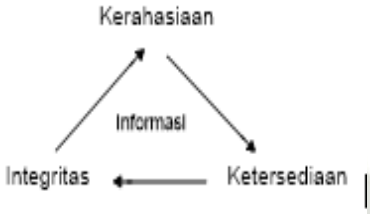
2.1.2 Aspek-Aspek Keamanan Informasi

Aspek keamanan informasi adalah aspek-aspek yang dilingkupi dan melingkupi keamanan informasi dalam sebuah sistem informasi. Aspek-aspek tersebut adalah (Sari, 2016):

1. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang-orang yang berwenang dan menjamin kerahasiaan data yang dikirm, diterima dan disimpan.
2. *Integrity* (integritas) aspek yang menjaminbahwa data tidak dirubah tanpa ada izin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan infor-

masi dan perangkat terkait.

Keamanan informasi diperoleh dengan mengimplementasikan seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan poranti lunak Gambar 2.1.



Gambar 2.1. Aspek Keamanan Informasi

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajeman sistem informasi memungkinkan data untuk didistribusi secara elekronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar.

2.1.3 Alasan Dibutuhkan Keamanan Informasi

Dengan meningkatnya transaksi dan tersedianya bermacam-macam teknik pemrosesan menggunakan komputer yang memungkinkan untuk berinteraksi dengan system lain,perusahaan mejadi sangat tergantung dengan komputerisasi. Di sisi lain dengan pesat lajunya teknologi,muncul risiko ancaman baru yang berkaitan degan komputerisasi.Pentingnya pengamanan yang efektif mulai diperhatikan oleh semua pihak.Semua pihak dapat memahami bahwa keamanan sistem informasi yang cukup andal sangat diperlukan.Perusahaan memiliki sederetan tujuan dengan diadakannya system informasi yang berbasis komputer di dalam perusahaan.Oleh karna itu,perusahaa menuntut agar diciptakan system keamanan terhadap *hardware* maupun *software*nya (Slamet, Wulandari, dan Amalia, 2019).

2.2 ISO 27001

Standar mutu internasional ISO 27001 adalah standar khusus *information technology* dibidang *information security management systems requirements*. Berdasarkan pengertiannya ISO 27001 adalah persyaratan untuk mendapatkan sertifikat keamanan informasi khususnya dibidang teknologi (aplikasi) serta umumnya standar teknologi ini menggunakan konsep *Plan¿Do¿Check¿*textitAction. Standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitkan pada mutu internasional ISO 27001 adalah standar khusus information bulan Oktober 2005 oleh

International Organization for Standarization dan International Electrotechnical Commission

2.3 Kerangka Kerja ISO 27001

Keamanan data informasi elektronik menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur penting. Sebab data/informasi adalah aset bagi perusahaan tersebut. Ancaman dan risiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya standar sistem manajemen keamanan informasi yang salah satunya adalah ISO 27001:2013. Dalam ISO ini dikenal standar penanganan risiko *(risk assessment)* yang melibatkan proses identifikasi risiko di mana setiap risiko yang ada harus dapat dikenal dengan baik, kemudian risiko dianalisis dampaknya dan dievaluasi cara-cara untuk menanggulangi risiko tersebut. Kerangka kerja ISO 27001 melibatkan proses komunikasi dan konsultasi serta pemantauan dan peninjauan untuk proses manajemen risiko. Proses penanganan risiko itu sendiri dijalan dalam empat tahapan proses secara berurutan yakni identifikasi, analisis, evaluasi dan penanganan risiko (Budiarto, 2017).Seperti pada Gambar 2.2

Gambar 2.2. Proses Manajeman Resiko dalam kerangka kerja ISO 27001

Penyusunan standar ini berawal pada tahun 1995, di mana sekelompok perusahaan besar yang terdiri dari *Board of Certification*, *British Telecom*, *Marks and Spencer*, *Midland Bank*, *Nationwide Building Society*, *Shell* dan *Unilever* bekerja sama untuk membuat suatu standar yang dinamakan *British Standard* 7799 (BS 7799) kemudian berkembang menjadi *The International Standards Organization* yang merupakan lembaga independen yang mengeluarkan standar operasional prosedur (SOP) terhadap kualitas suatu layanan. ISO memperkenalkan ISO 27001:2013 yang berisi standar mengenai manajemen informasi yang terakhir kali di perbarui pada tahun 2013.

2.4 Indeks Keamanan Informasi(KAMI)

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi ?(Informasi, 2012)). Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh Instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan snapshot indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait *(steakholders)*. Penggunaan dan publikasi hasil evaluasi indeks KAMI merupakan bentuk tanggung jawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antara pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari *lesson-learned* yang sudah dilalui.

2.4.1 Metode Penilaian Indeks KAMI

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area di bawah ini:

1. Tata Kelola Keamanan Informasi Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

2. Pengelolaan Risiko Keamanan Informasi Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi
3. Kerangka Kerja Keamanan Informasi Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
4. Pengelolaan Aset Informasi Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
5. Teknologi dan Keamanan Informasi Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Penyusunan kembali menjadi lima komponen ini dilakukan untuk mendapatkan bentuk evaluasi mandiri yang mudah untuk ditanggapi diaman hasil evaluasinya sendiri nanti akan dapat digunakan sebagai panduan pembenahan atau peningkatan kinerja tata kelola keamanan informasi.

2.4.2 Proses Penilaian Kelengkapan dan Kematangan Tata Kelola Keamanan Informasi

1. Jumlah (kelengkapan) bentuk pengamanan Metode pertama akan mengevaluasi sejauh mana instansi responden sudah merapkan pengamana sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Untuk kelima area evaluasi, yang dimaksud sebagai kontrol dijelaskan secara singkat dibawah ini:
   (a) Tata Kelola Keamanan Informasi Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung jawab, kewenangan pengelolaan keamanan informasi, dari pimpinanunit kerja sampai ke pelaksana operasional. Termasuk dalam area ini juga adalah adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi penigkatan kerja tata kelola keamanan informasi.
   (b) Pengelolaan Resiko Keamanan Informasi Bentuk tata kelola yang diperlakukan adalah adanya kerangka kerja pengelolaan resiko dengan definisi yang eksplisit terkait ambang batas diterimanya resiko, program pengelolaan resiko dan langkah mitigasi yagn secara regular dikaji efektifitasnya.
   (c) Kerangka Kerja Keamana Informasi Kelengkapan kontrol di area ini memerlukan sejumlah kebijakan dan prosedur kerja operasional, ter-

masuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.

(d) Pengelolaan Aset Informasi Kontrol yang diperlukan dalam area ini adalah bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.

(e) Teknologi dan Keamanan Informasi Untuk kepentingan indeks KAMI, aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan resiko, dan tidak secara eksplisit menyebutkan teknologi atau pabrikan tertentu.

2. Tingkat Kematangan Proses Pengelolaan Pengamanan Informasi Metode yang kedua merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasiyang mengacu pada tingkatan kematangan yang digunkan oleh kerangka kerja COBIT (Control Objective for Information and related Technology) atau CMMI (Capability Maturity Model for Integration). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementrian/Lembaga. Pemetaan dan pemeringkatan akan dilakukan ole tim yang telah ditentukan oleh Kementrian Komunikasi dan Informasi(Kominfo) dan menjadi dasar bagi pemberian OPINI kominfo tentang kondisi tata kelola keamanan informasi di Kementrian/Lembaga terkait. Untuk keperluan indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai berikut:

(a) Tingkat 0- Tidak diketahui (PASIF)
   i. Status Kesiapan Keamanan informasi tidak diketahui
   ii. Pihak yang terlibat tidak mengetahui atau tidak melaporkan pemeringkatan indeks KAMI.

(b) Tingkat I- kondisi Awal(REAKTIF)
   i. Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.
   ii. Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluru resiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
   iii. Kelemahan teknis dan nonteknis tidak terindikasi dengan baik.
   iv. Pihak yang terlibat tidak menyadari tanggung jawab mereka.

(c) Tingkat II- Penerapan Kerangka Keja Dasar (AKTIF)
   i. Pengamanan sudah diterapkan walaupun sebagaian besar masih

diarea teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang aktif.

ii. Proses pengamanan berjalan tanpa adanya dokumentasi atau rekam resmi.

iii. Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.

iv. Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektifitasnya.

v. Kelemahan dalam menajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.

vi. Menajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.

vii. Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

(d) Tingkat III- Terdefinisi dan Konsisten (PRO AKTIF)

i. Bentuk pengamanan yang baku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.

ii. Efektivitas pengamanan dievaluasi secara berkala, walaupun belum melalui proses yang terstruktur.

iii. Pihak pelaksana dan pimpinan secara umum dapat menangani permasalahan terkait pengelolaan keamanan pengendalian dengan tepat, akan tetapi beberapa kelemahan dalam sistem manajemen masih ditemukan sehingga dapat mengakibatkan dampak yang signifikan.

iv. Kerangka kerja pengamanan sudah memenuhi ambang batas minimun standar atau persyaratan hukum yang terkait.

v. Secara umum semua pihak yang terlibat menyadari tanggung jawab mereka dalam pengamanan informasi.

(e) Tingkat IV- Terkelola dan Terstrukur (TERKENDALI)

i. Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen resiko.

ii. Evaluasi (pengukuran) pencapaian sasaran keamanan dilakukan secara rutin, formal dan terdokumentasi.

iii. Penerapan pengamanan teknis secara konsisten dievaluasi efektifitasnya.

iv. Kelemahan manajemen pengamanan teridentifikasi dengan baik dan secara konsisten ditindak lanjuti pembenahannya.
v. Menajemen pengamanan bersifat pro-aktif dan menerapkan pembenahan untuk mencapai bentuk pengelolaan yang efisien.
vi. Insiden dan tidak patuh (non-conformity) diselesaikan melalui proses formal dengan pembelajaran akar permasalahan.
vii. Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.

(f) Tingkat V- Optimal (OPTIMAL)

i. Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan resiko yang terstruktur.
ii. Pengamanan informasi dan manajemen resiko sudah terintegrasi dengan tugas pokok instansi.
iii. Kinerja pengamanan dievaluasi secara kontinyu, dengan analisis parameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja.
iv. Target pencapaian program pengamanan infromasi selalu dipantau, dievaluasi dan diperbaiki.
v. Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan.

2.4.3 Petunjuk Penggunaan Alat Evaluasi Indeks Keamanan Informasi (Indeks KAMI)

Secara umum, peoses penilaian menggunakan KAMI dapat dilihat pada Gambar 2.3 dibawah ini. Melalui ilustrasi gambar berikut, dapat dilihat bahwa indeks KAMI adalah perangkat untuk mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapam secara berkala. Apabila terjadi perubahan pada infrastruktur atau unit kerja yang dalam lingkup awal evaluasi indeks KAMI, pengkajian ulang bermanfaat untuk memastikan kelengkapan dan kematangan bentuk tata kelola yang diterapkan di awal. Ilustrasi tampilan informasi dapat dilihat pada berikut:

Gambar 2.3. Ilustrasi Tampilan Evaluasi

1. **Ruang lingkup**

Langkah pertama yang harus dilakukan adalah mendefinisikan ruang lingkup penilaian. Ruang lingkup dapat dipilih sesuai dengan kepentingan penilian indeks KAMI, dan dapat dipilih sebagai suatu satuan kerja (ditingkat apapun) ataupun suatu sistem informasi

2. **Peran TIK**

Sebelum proses penilaian dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap peran TIK dalam instansi atau cakupan evaluasinya, Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah unutk mengelompokan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang sama. Peran TIK dievaluasi dengan bahasan:

(a) Total anggaran tahunan yang di alokasikan untuk TIK.

(b) Jumlah staf atau pengguna dlam instansi yang menggunakan infrastruktur TIK.

(c) Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi instansi anda.

(d) Nilai kekayaan intelektuan yang dimiliki dan dihasilkan oleh instansi anda.
(e) Dampak dari kegagalan sistem TIK utama yang digunakan instansi anda.
(f) Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja instansi anda.
(g) Dampak dari kegagalan sistem TIK instansi anda terhadap kinerja instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional.
(h) Tingkat sensitifitas pengguna sistem TIK di instansi anda.
(i) Tingkat kepatuhan terhadap UU dan pernagkat hukum lainnya.
(j) Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK instansi anda.
(k) Tingkat ketergantunngan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK
(l) Tingkat klasifikasi/kekritisan sistem TIK d instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi

Kategori peran TIK yagn dimaksud disini secara umum dapat dijelaskan sebagai beikut:

(a) Minim Pengguna TIK dalam lingkup yang didefinisikan tidak signifikan, dan keberadaannya tidak berpengaruh proses kerja yang berjalan.
(b) Rendah Pengguna TIK mendukung proses kerja yang berjalan, walaupun tidak pada tingkatan yang signifikan.
(c) Sedang Pengguna TIK merupakan bagian dari proses kerja yang berjalan, akan tetapi ketergantungannya masih terbatas.
(d) Tinggi TIK merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan.
(e) Kriitis Pengguna TIK merupakan satu-satunya cara untuk menjalankan proses kerja yang bersifat strategis atau berskala nasional.

3. **Proses Penilaian** Seluruh pertanyaan yang ada dalam setiap area dikelompokan menjadi 3 kategori pengamanan, sesuai dengan tahapan dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja dasar keamanan informasi masuk dalam kategori “I”, unutk efektifitas dan konsistensi penerapannya didefinisikan sebagai kategori “2”, dan hal-hal yang merujuk pada kemampuan unutk selalu meningkatkan kiner-

ja keamanan informasi adalah kategori"3". Responden kemudian diminta unutk menjawab setiap pertanyaan dengan pilihan Status Penerapan:

(a) Tidak Dilakukan;
(b) Dalam Perencanaan;
(c) Dalam Pernecenaan atau DiterapkanSebagian;
(d) Diterapkan Secara Menyeluruh.

Setiap jawaban akan diberikan skor yang nilainya disusaikan dengan tahapan penerapan(kategori) bentuk pengamanan. Unutk tahapan awal nilainya akan lebih rendah dibandingkan tahapan berikutnya. Demikiana halnya unutk status penerapannya, penerapan yang sudah berjalan secara menyeluruh memberikan nilai yang lebih tinggi dibandingkan bentuk penerapan lainnya. Tabel pemetaan skor dapat dilihat pada. Tabel 2.1 ini merangkum seluruh jumlah jawaban penilaian mandiri dan membentuk matriks antara status pengamanan dan kategori.

Tabel 2.1. Pemetaan Skor

Status Pengamanan	Kategori Pengamanan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan Secara Menyeluruh	3	6	9

Nilai unutk kategori pengamanan yang tahapannya lebih awal, lebih rendah dibandingkan dengan nilai untuk tahap selanjutnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan kategori "3" hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan kategori "I"dan "2" sudah diisi dengan status minimal "Diterapkan Sebagian".

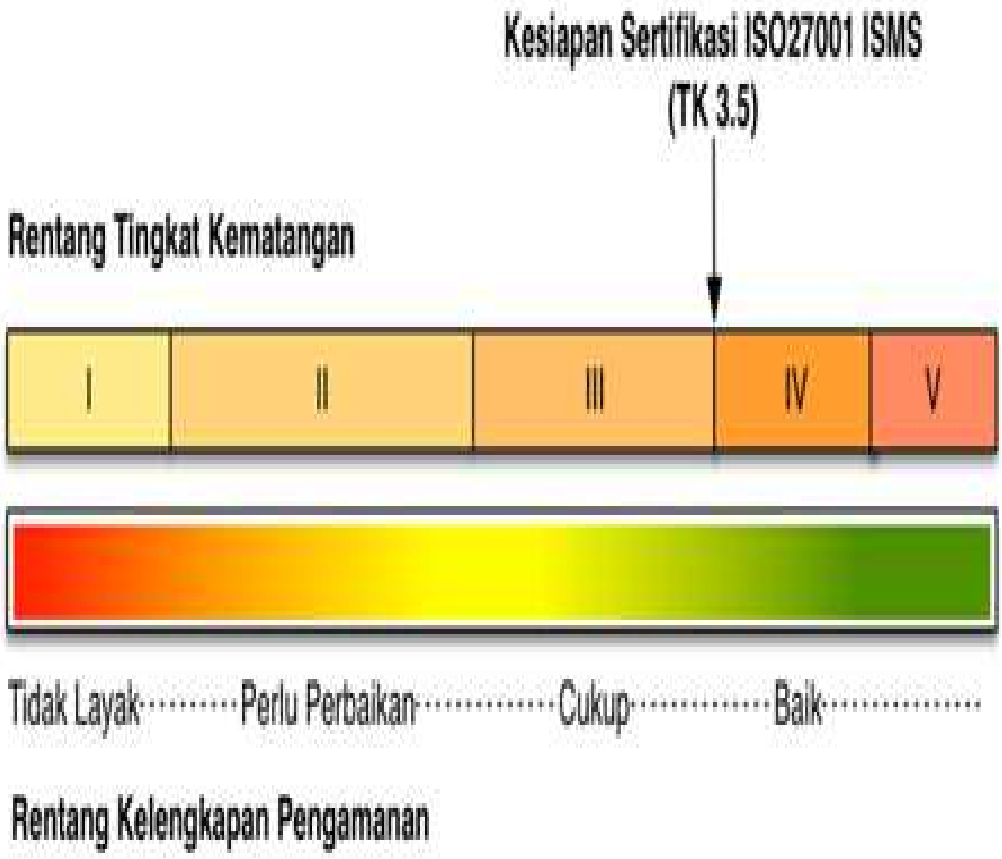
4. **Pengkajian Hasil Indeks KAMI** Hasil dari penjumlahan skor masing-masing area ditampilkan dalam 2 instrumen di dasbor:

(a) Tabel nilai masing-masing area
(b) *Radar Chart* dengan 5 (lima) sumbu sesuai dengan area pengamanan Untuk nilai masing-masing area dirangkum dalam Tabel 2.2 Pada tabel ini, institusi akan melihat seberapa besar tingkat kelengkapan masing-masing area yang telah dicapai.

Tabel 2.2. Rangkuman Evaluasi Berdasarkan Area Keamanan Informasi

Area Keamanan Informasi	Nilai
Peran/Tingkat Kepentingan TIK	0
Tata Kelola	0
Pengelolaan Resiko	0
Kerangka Kerja Keamanan Informasi	0
Pengelolaan Aset	0
Teknologi Keamanan Informasi	0

Jumlah (nilai) yang dihasilkan kemudian dipetakan sesuai dengan tingkat kepentingan TIK terhadap cakupan instansi tersebut. Status kesiapan yang dicapai merupakan kondisi yang dilaporkan sepeti pada Gambar 2.4



Gambar 2.4. Rentang Tingkat Kematangan

Tabel 2.3. Matriks Peran TIK dan Status Kesiapan

Skor bagian I		Skor Bagian II+III+IV+V+VI		Status Kesiapan
Rendah				
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang				
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi				
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis				
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

Tabel 2.3 menggambarkan bahwa semakin tinggi ketergantungan terhadap TIK atau semakin penting peran TIK terhadap tugas instansi tersebut, maka semakin banyak bentuk pengamanan yang diperlukan, dan yang harus diterapkan sampai tahap tertinggi.

2.4.4 RSUD ARIFIN ACHMAD Pekanbaru

1. **Visi**

   Menjadi rumah sakit pendidikan mandiri dengan pelayanan paripurna yang memenuhi standar internasional

2. **Misi**

(a) Menyelenggarakan fungsi pelayanan kesehatan sesuai dengan standar internasional dan menjadi pusat rujukan bagi rumah sakit lainnya di provinsi Riau.

(b) Melaksanakan fungsi sebagai rumah sakit pendidikan kedokteran dan kesehatan lainnya.

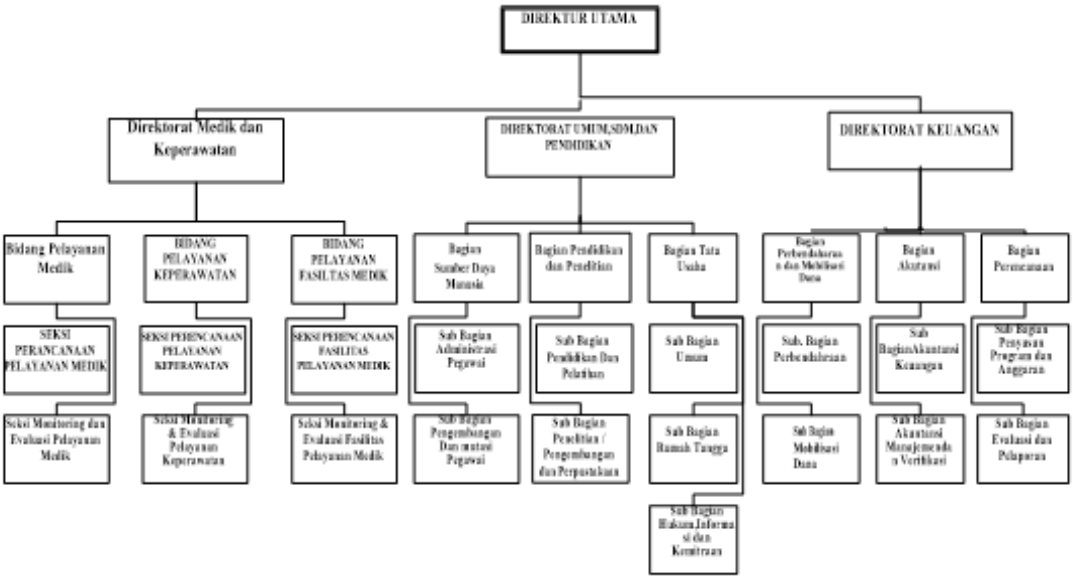
(c) Melaksanakan fungsi administrasi secara profesional.

3. **Motto**

   Kepuasan adalah kebahagiaan kami.

4. **Struktur Organisasi**

   Dapat dilihat pada Gambar 2.5



Gambar 2.5. Rentang Tingkat Kematangan

2.5 Penelitian Terdahulu

Pada penelitian ini, penelitian terdahulu yang peneliti gunakan sebagai acuan dan referensi diantaranya penelitian yang dilakukan oleh Fairzah A Basyarahil pada tahun 2017 yang membahas tentang "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya" di ketahui bahwa hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar 249 dari jumlah total keseluruhan sebesar 645 dan berada pada level I-II dimana level ini masih berada pada kondisi awal penerpan keamanan informasi dan kondisi penerapan kerangka kerja dasar penerapan keamanan informasi, Tingkat kematangan per-area akan didapatkan bahwa Area Tata Kelola Keamanan Informasi berada pada tingkat I+, area Pengelolaan Risiko Keamanan Informasi pada tingkat I, area Kerangka kerja Pengelolaan Keamanan Informasi pada tingkat I+, area Pengelolaan Aset Informasi pada tingkat I+, dan area Teknologi & Keamanan Informasi pada tingkat II.

Penelitian selanjutnya yang menggunakan standar ISO 27001:2013 dalam mengevaluasi keamanan informasi adalah penelitian yang dilakukan oleh Edo Riky Pratama,dkk pada tahun 2018 yang membahas tentang "Evaluasi Tata Kelola Sistem

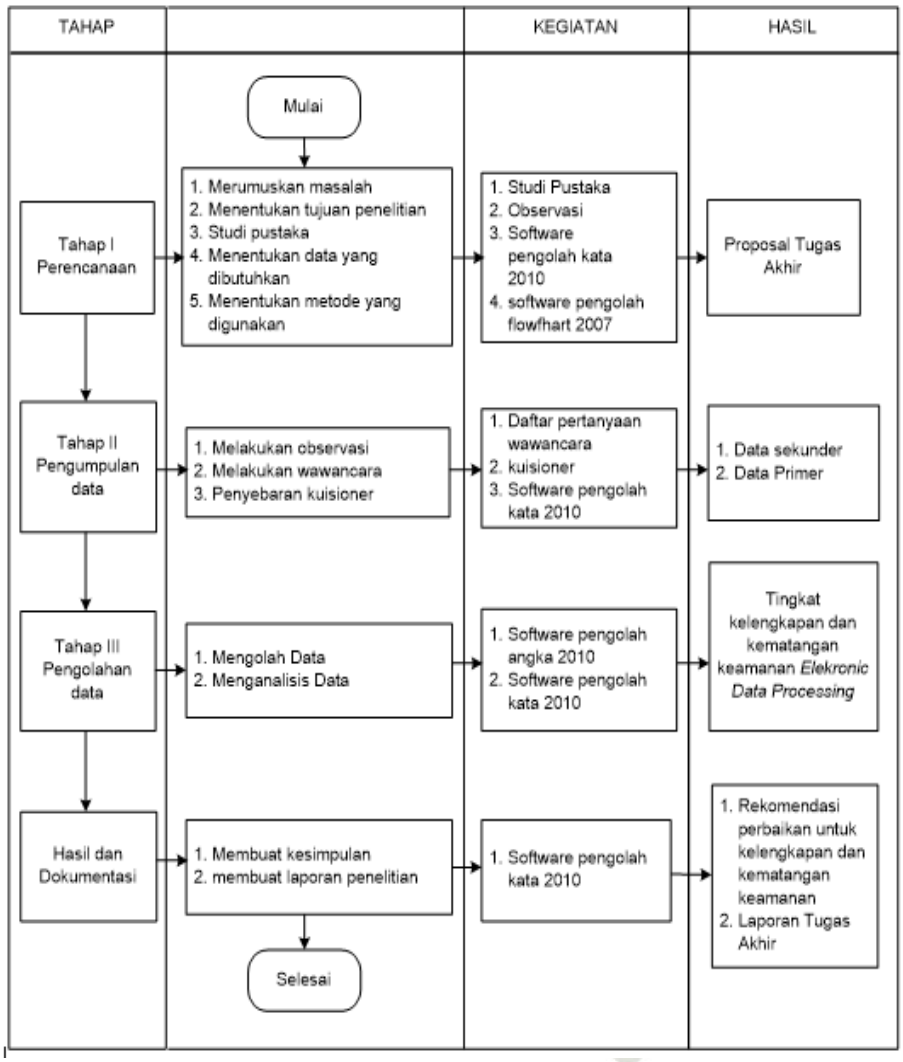
Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur) diketahui bahwa Tingkat kelengkapan dan kematangan keamanan informasi KOMINFO masih rendah. penyebab rendahnya tingkat kelengkapan dan kematangan keamanan informasi ini adalah KOMINFO belum menerapkan semua syarat keamanan informasi atau masih dalam perencanaan. Rendahnya tingkat kelengkapan ini ditunjukan oleh bar chart yang menunjukan warna merah dengan total nilai 245, yang artinya keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur tidak layak dan butuh perbaikan. Sedangkan tingkat kematangan setiap area keamanan informasi berada pada I+.

Kemudian penelitian yang dilakukan oleh Muhammad Ramadhan Slamet pada tahun 2019 yang berjudul "Penilaian Pengamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam" diketahui bahwa tingkat kematangan pengamanan teknologi total skor yang didapatkan adalah 65 atau 54,17% dari total skor maksimum. Oleh sebab itu, tingkat kematangan pengamanan teknologi berada pada tingkat kematangan II yang berarti tingkat kematangan pengamanan teknologi sistem elektronik (sistem pembelajaran elektronik) Politeknik Negeri Batam (Polibatam) di bawah tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi, yaitu III+ khususnya jika dilhat dari perspektif pengamanan teknologi. Hal ini disebabkan posisi Polibatam masih dalam tahap pengembangan organisasi. Selain itu, fokus organisasi masih terkait hal-hal operasional, belum bersifat strategis.

BAB 3
METODOLOGI PENELITIAN

3.1 Metodologi Penelitian Tugas Akhir

Terdapat beberapa tahap yang peneliti lakukan pada penelitian ini. Adapun metodologi penelitian yang dilakukan dapat dilihat pada Gambar 3.1



Gambar 3.1. Metodologi Penelitian

3.2 Tahap Perencanaan

Langkah pertama dilakukan adalah memilih dan merencanakan apa yang akan diteliti, merumuskan masalah yang akan diteliti serta menentukan tujuan dalam melakukan penelitian. Kemudian menentukan data data serta informasi akurat yang dibutuhkan dalam penelitian.

3.3 Tahap Pengumpulan Data

Tahap pengumpulan data merupakan tahapan yang dilakukan untuk memperoleh informasi yang dibutuhkan dalam proses penelitian. Langkah-langkah yang dilakukan adalah:

3.3.1 Menentukan Masalah

Dalam langkah ini yang dilakukan adalah melakukan wawancara kepada kepala bagian *Electronic Data Processing* (EDP) kemudian mencatat masalah yang terjadi pada EDP. Hasil wawancara menjelaskan bahwa saat ini semakin berkembangnya teknologi yang digunakan semakin banyak informasi penting dan berharga yang diolah oleh EDP. Tetapi hingga saat ini belum adanya evaluasi yang dilakukan oleh RSUD Arifin Achmad terutama tentang keamanan sistem informasi pada EDP. Sehingga belum diketahuinya apakah proses pada EDP sudah dilakukan berdasarkan standar ISO.

3.3.2 Menentukan Tujuan Penelitian

Penentuan tujuan penelitian berfungsi untuk memperjelas apa saja yang menjadi sasaran dari penelitian ini yaitu untuk mengetahui tingkat kelengkapan dan kematangan keamanan informasi pada RSUD Arifin Achmad Pekanbaru khususnya keamanan informasi pada bagian *Electronic Data Processing* (EDP).

3.3.3 Studi Pustaka

Studi pustaka tidak terlepas dari literatur-literatur ilmiah sehingga studi kepustakaan merupakan hal yang penting untuk dilakukan dalam penelitian. Dalam penelitian ini studi pustaka dilakukan dengan mecari jurnal-jurnal atau skripsi dan buku yang membahas mengenai model penelitian menggunakan UTAUT.

3.3.4 Menentukan Data Yang Dibutuhkan

Pada penelitian ini data yang dibutuhkan yaitu:

1. Data Primer

   Data primer adalah data yang diperoleh langsung dari sumber aslinya, meliputi:

   (a) Data dari RSUD Arifin Achmad Pekanbaru seperti sejarah dan struktur organisasi
   (b) Data yang didapat langsung dari hasil wawancara
   (c) Data yang didapat dari lembar pengisian kuisioner indeks KAMI
   (d) Data observasi

2. Data Sekunder

   Data sekunder adalah data yang diperlukan sebagai data pendukung dari

data primer. Adapun data yang diperoleh penulis berasal dari buku-buku dan jurnal yang berhubungan dengan teori-teori tentang pengukuran keamanan informasi berstandar ISO 27001.

3.3.5 Menentukan Metode Yang Digunakan

Metode yang digunakan pada penelitian ini disesuaikan dengan masalah peneliti yaitu masalah keamanan informasi. Pada penelitian ini metode yang digunakan adalah pengukuran dengan indeks Keamanan Informasi (KAMI). Untuk mengetahui tingkat keamanan informasi pada *Electronic Data Processing* (EDP) di RSUD Arifin Achmad Pekanbaru.

3.4 Tahap Pengumpulan Data

Pada tahap pengumpulan data penulis melakukan proses dengan alat bantu pengumpulan data yaitu;

1. Observasi Dalam penelitian ini peneliti melakukan pengamatan langsung di lingkungan RSUD Arifin Achmad Pekanbaru. Dari hasil observasi diperoleh bahwa belum pernah dilakukannya pengukuran terhadap keamanan informasi dan tidak diketahui seberapa besar tingkat kelengkapan dan kematangan keamanan informasi pada EDP.
2. Wawancara Dalam penelitian ini peneliti melakukan wawancara kepada kepala bagian Electronic Data Processing (EDP) mengenai keamanan informasi. Proses memeroleh data dengan cara tanya jawab secara langsung sehingga didapatkan data yang berkualitas.
3. Penyebaran Kuisioner Peneliti menyebarkan kuisioner yang berisi pertanyaan-pertanyaan secara tertulis untuk diisi oleh sumber informasi. Kuisioner disebarkan kepada seluruh staff bagian EDP. Pernyataan-pernyataan kuisioner sesuai pada dimensi indeks KAMI yang dirancang untuk mengetahui tingkat keamanan informasi.

3.5 Tahap Pengolahan Data

Tahap pengolahan data dapat dilakukan ketika data yang diperlukan sudah didapatkan. Pada tahap ini kegiatan yang dilakukan adalah melakukan pengukuran terhadap keamanan informasi pada EDP RSUD Arifin Achmad Pekanbaru. Hal yang pertama dilakukan adalah mengolah data yang diperoleh dari hasil pengisian kuisioner oleh staff EDP berdasarkan kerangka kerja yang terdapat pada indeks Keamanan Informasi (KAMI). Dari hasil pengolahan data nanti akan diketahui tingkat kematangan informasi pada EDP RSUD Arifin Achmad Pekanbaru. Hasil dari pengolahan data inilah yang akan dijadikan bahan acuan untuk pemberian

rekomendasi kepada pihak EDP RSUD Arifin Achmad Pekanbaru. Alur yang dilakukan dalam pengukuran indeks KAMI dapat dilihat sebagai berikut:

1. Mendifinisikan Ruang Lingkup
2. Menetapkan Peran atau Tingkat Kepentingan TIK di Instansi
3. Menilai Kelengkapan Pengamanan 5 Area
4. Mengkaji Hasil Indeks KAMI disertai dengan menetapkan langkah-langkah perbaikan. Tingkat kesiapan keamanan informasi dibagi menjadi empat tingkatan. Jika hasil tingkat kepentingan TIK mendapat nilai rendah, maka semakin rendah pula batasan yang harus dicapai organisasi tersebut dalam penilaian lima bagian indeks KAMI, dan sebaliknya. Keempat tingkatan tersebut dapat dilihat pada Tabel 3.1dibawah ini.

Tabel 3.1. Peran TIK

Rendah		Indeks(Skor Akhir)		Status Kesiapan
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		Indeks(Skor Akhir)		Status Kesiapan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Indeks(Skor Akhir)		Status Kesiapan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup

Dalam penilaian tingkat peran TIK, terdapat lima pilihan jawaban yang dapat dilihat pada Tabel 3.2.

Tabel 3.2. Pilihan Jawaban

Jawaban	Nilai
Minimal	0
Rendah	1
Sedang	2
Tinggi	3
Kritis	4

3.6 Hasil dan Dokumentasi

Tahap ini mengumpulkan dan menyusun setiap tahapan yang telah dilakukan serta menyusun penemuan-penemuan berdasarkan batasan penelitian yang ada, dan membuat kesimpulan serta menyajikan saran karena penelitian yang dibuat memiliki keterbatasan ataupun asumsi-asumsi. Seluruh hasil penelitian dibuat dalam laporan tertulis Tugas Akhir dengan teknik mengikuti format dan penulisan laporan tugas akhir pada UIN SUSKA Riau. Hasil dokumentasi dapat dijadikan sebagai rekomendasi terhadap tingkat keamanan dan kematangan informasi berdasarkan hasil penelitian yang telah dilakukan.

BAB 5
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil pengolahan dan pembahasan kuisioner didapatkan kesimpulan :

1. Hasil evaluasi akhirpada tingkat kelengkapan penerapan standar keamanan dengan skor 308 dari skor maksimal yaitu 645 yang berada pada tingkat keamanan “Tidak Layak”.Untuk melihat detail tingkat kematangan kelima area dapat dilihat pada tabel 4.7.
2. Hasil dari evaluasi tugas akhir ini membuktikan bahwa instansi membutuhkan perbaikan dan membuat kebijakan baru dalam pengelolaan keamanan system informasi SIMRS untuk menjadi lebih baik.Rekomendasi yang telah peneliti buat dapat dilihat pada tabel 4.8.

5.2 Saran

Saran yang dapat diambil dari hasil pengerjaan tugas akhir dengan studi kasus Evaluasi Keamanan Informasi Pada RSUD Arifin Achmad dengan Menggunakan Indeks Keamanan Informasi (KAMI) ini adalah sebagai berikut:

1. Pihak EDP RSUD Arifin Achmad sudah sangat baik dalam kesadaran tata kelola dan pengelolaan asset informasi, hanya tinggal menerapkan segala kebijakan dan peraturan yang telah dibuat secara berkelanjutan
2. Harus lebih diperhatikannya lagi bagian pengelolaan resiko karena masih banyaknya kajian risiko yang tidak dilakukan.
3. Alangkah lebih baikya jika mengikuti petunjuk teknis secara detail dengan megikuti acara Bimbingan Teknis yang diadakan oleh pihak Kominfo mengenai proses penilaian pada Indeks KAMI guna memahami perolehan skor yang didapat maupun untuk perbaikan serta pengembangan proses penilaian untuk kedepannya.
4. Perlu dibuatnya suatu instrument penilaian yang baru, karena indeks KAMI saat ini masih menyesuaikan dengan standar ISO 27001 tahun 2015. Sedangkan saat ini sudah terdapat ISO 27001 tahun 2019

DAFTAR PUSTAKA

Andress, J. (2014). *The basics of information security: understanding the fundamentals of infosec in theory and practice*. Syngress.

Basyarahil, F. A., Astuti, H. M., Hidayanto, B. C., dkk. (2017). *Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (kami) berdasarkan iso/iec 27001: 2013 pada direktorat pengembangan teknologi dan sistem informasi (dptsi) its surabaya* (Unpublished doctoral dissertation). Sepuluh Nopember Institute of Technology.

Budiarto, R. (2017). Manajemen risiko keamanan sistem informasi menggunakan metode fmea dan iso 27001 pada organisasi xyz. *Computer Engineering, Science and System Journal*, *2*(2), 48-58.

Informasi, T. (2012). *Panduan penerapan tata kelola keamanan informasi bagi penyelenggara pelayanan publik*. Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika.

Pratama, Edo Rizky. "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)". *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. Vol. 2, No.11. 2018.

Sari, Linda Permata. "Pengukuran Tingkat Kematangan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Ptipd UIN SUSKA RIAU". *Skripsi*. Fakultas Sains dan Teknologi. 2016.

Sarno, R dan Iffano,I. "Sistem Manajeman Keamanan Informasi". Penerbit ITS Press, Surabaya.2009.

Slamet, Muhammad Ramadhan, dkk. "Penilaian Pengamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam". *Journal of Business Administration*. Vol. 3, No.1. 2019.

Sutabri, Tata. "Konsep Sistem Informasi".Andi Offset, Yogyakarta. 2012.

T.D.K. Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik,". Jakarta, Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, 2012, pp. 34 - 58.

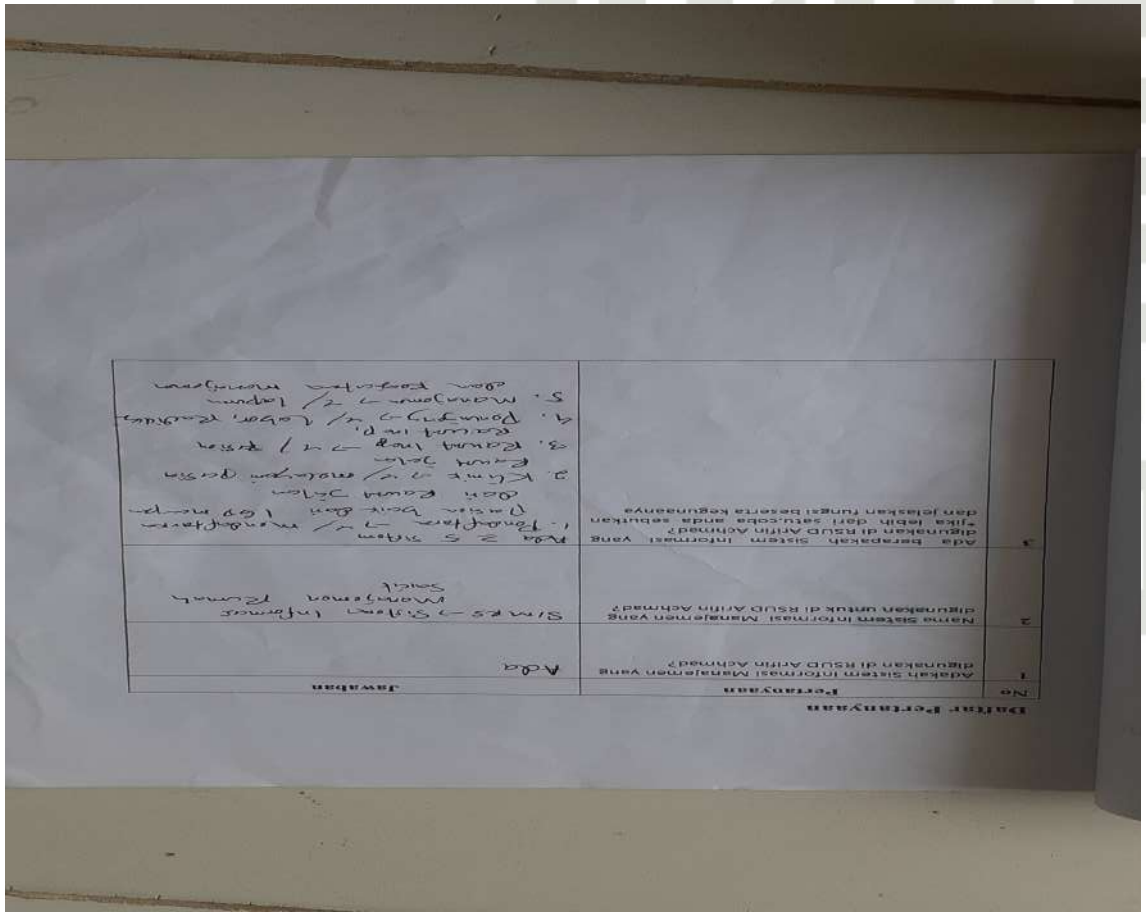
Whitman, Michael E dan Mattord Herbert J. "*Priciples of Information Security. USA: Course Technology*".2011.

LAMPIRAN A
HASIL WAWANCARA

BIODATA NARASUMBER

Identitas Instansi Pemerintah	RSUD Arifin Achmad
Alamat	Jl. Diponegoro No. 2
Nomor Telpon	
Email	dsp. rsudaa@gmail.com
Narasumber	
NIP	
Jabatan	
Tanggal Pengisian	30 - 10 - 2019
Deskripsi Ruang Lingkup	Instalasi EDP / Elektrumt Data Processing
Isi dengan deskripsi ruang lingkup instansi (satuan kerja) dan infrastruktur TIK	

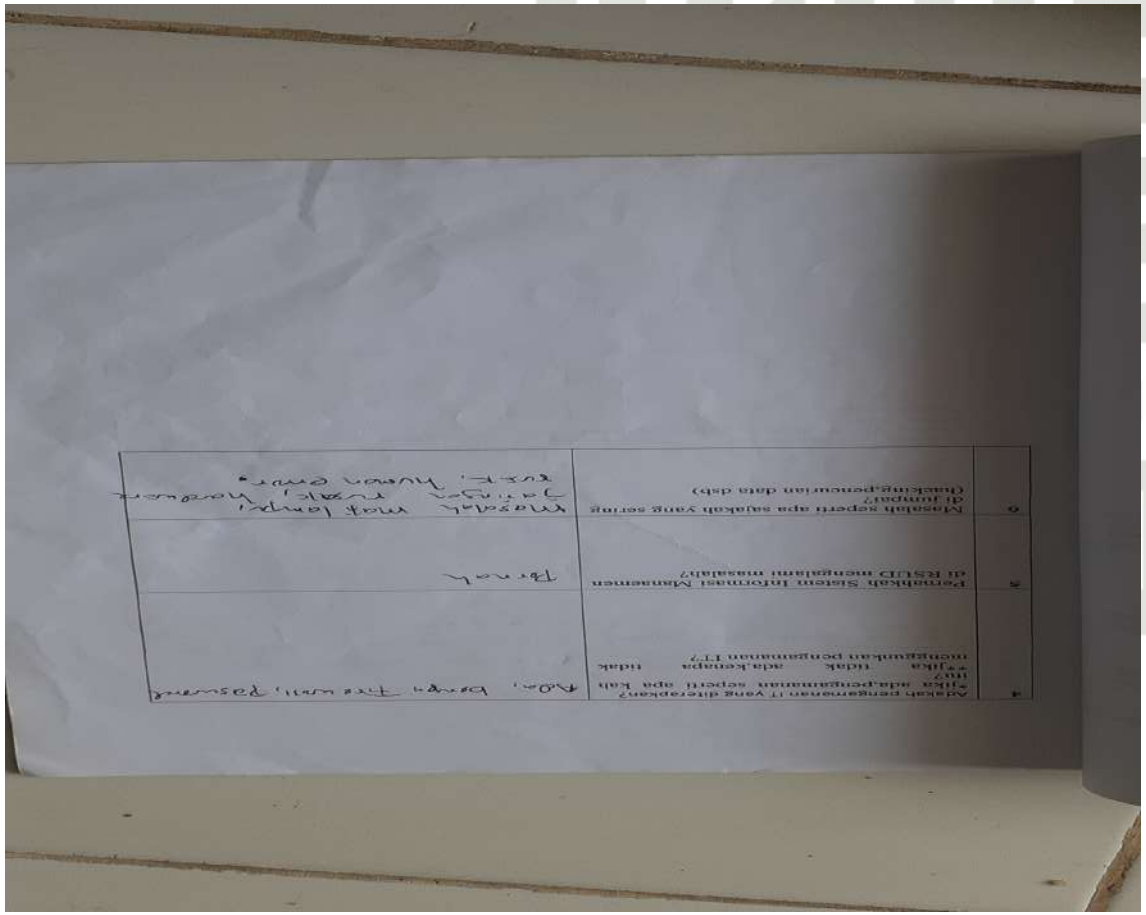
Gambar A.1. Lampiran Wawancara 1



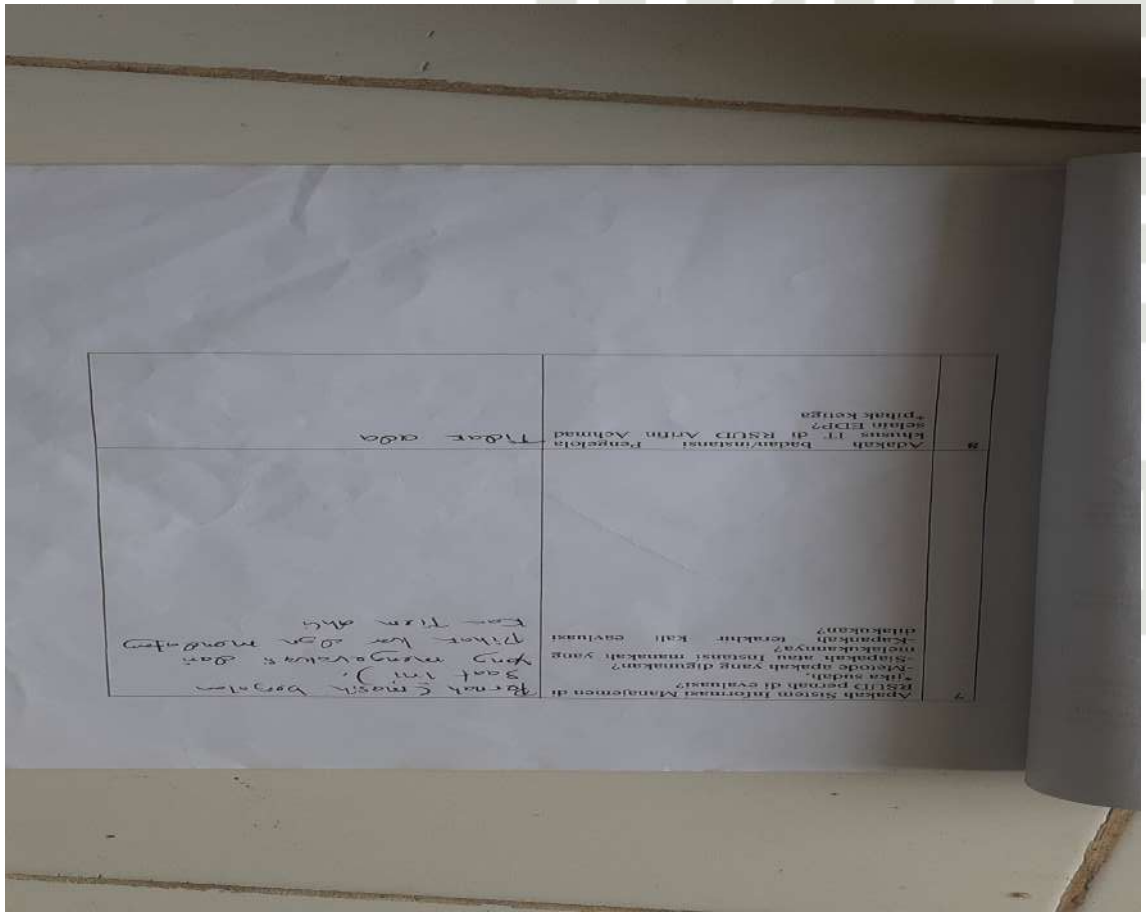
Daftar Pertanyaan

No	Pertanyaan	Jawaban
1	Adakah Sistem Informasi Manajemen yang di gunakan di RSUD Arifin Achmad?	Ada
2	Nama Sistem Informasi Manajemen yang di gunakan untuk di RSUD Arifin Achmad?	SIMRS - Sistem Informasi Manajemen Rumah Sakit
3	Ada berapakah Sistem Informasi yang di gunakan di RSUD Arifin Achmad? jika lebih dari satu,coba anda sebutkan dan jelaskan fungsi beserta kegunaanya	Ada 3 Sistem 1. Pendaftaran - Untuk mendaftarkan Pasien Baru dan Lama 2. Kasir - Untuk melayani pembayaran Rawat Jalan 3. Rawat Inap - Untuk Rawat Inap, Rawat Jalan 4. Poli gigi - Untuk Lobar, Rawat Jalan 5. Manajemen - Untuk Laporan dan Pengarsipan Manajemen

Gambar A.2. Lampiran Wawancara 2



Gambar A.3. Lampiran Wawancara 3



Gambar A.4. Lampiran Wawancara 4

Identitas Instansi Pemerintah	RSUD Arifin Achmad
Alamat	Jl. Diponegoro No.2
Nomor Telpon	
Email	edp.rsudpku@gmail.com
Pengisi Lembar Evaluasi	
NIP	
Jabatan	
Tanggal Pengisian	30 - 10 - 2023
Deskripsi Ruang Lingkup	Instalasi EDP/elektronik Data Processing
Isi dengan deskripsi ruang lingkup instansi (satuan kerja) dan infrastruktur TIK	

Gambar A.5. Lampiran Wawancara 5

Wawancara

Narasumber : Ike Emanarni
Jabatan : Administrasi EDP
Waktu : 22 Juli 2020
Lokasi : Kantor EDP RSUD Arifin Achmad

Hasil Wawancara

Pertanyaan : **Apa Fungsi dan Tugas Pokok EDP ?**

Jawaban :

Memberikan Pelayanan Terhadap Kebutuhan TI RSUD Arifin Achmad Khususnya SIMRS guna menghadirkan pelayanan rumah sakit yang cepat, tepat dan akurat yang didukung dengan penggunaan sistem informasi.

Pertanyaan :**Apakah RSUD Arifin Achmad sudah memiliki Master plan maupun SOP yang menunjang kinerja EDP ?**

Jawaban :

RSUD belum memiliki master plan dan sop. Selama ini segala prosedural dan pemenuhan kebutuhan RSUD bergantung kepada Vendor. Sehingga, penanganan masalah TI yang terjadi di rumah sakit oleh pihak EDP menjadi rumit.

Pertanyaan : **Bagaimana dengan SDM yang ada di EDP, Berapa jumlahnya dan apakah mampu menunjang seluruh kebutuhan TI RSUD khususnya SIMRS ?**

Jawaban :

SDM yang ada dirasa belum memadai dan hanya sebatas support. Jumlah personel 7 orang, yang dirasa kurang dalam mensupport keseluruhan rumah sakit.

Gambar A.6. Lampiran Wawancara 6

Pertanyaan : **Apakah yang dilakukan RSUD khususnya EDP dalam mengatasi kekurangan personel?**

Jawaban :
-

Pertanyaan : **Apa saja masalah yang ditemukan dilapangan berkaitan dengan TI khususnya SIMRS?**

Jawaban :

- Banyaknya permintaan sesaat yakni permintaan dari user (staf lain)
- kurang disiplinnya pengguna SIMRS. Contoh, pasien sudah pulang secara fisik namun secara sistem masih terdata sebagai pasien sehingga pada saat si pasien melakukan kontrol justru masih terdata sebagai pasien rawat inap.

Pertanyaan : **Bagaimana RSUD khususnya EDP memanajemen masalah?**

Jawaban :

Tidak ada manajemen masalah secara spesifik, evaluasi maupun upaya peningkatan sdm user berupa pelatihan. Untuk edukasi hanya bersifat pemberitahuan atau pendekatan perseorangan. Untuk pelatihan staf EDP sendiri hanya sebatas penanganan masalah yang ditemukan di lapangan dan tidak pernah diikut sertakan dalam training yang spesifik mengenai TI.

Pertanyaan : **Aplikasi apa saja yang ada pada simrs saat ini?**

Jawaban :

Rekam medis, instalasi rawat inap, rawat darurat, rawat jalan, farmasi, kasier, penjulan obat, bedah sentral, radiologi, patologi, rehab medis, bank darah, gizi, akuntansi, keuangan, logistik, perbendaharaan, sdm, asuhan keperawatan

Gambar A.7. Lampiran Wawancara 7

Pertanyaan : **Adakah aplikasi yang belum digunakan pada simrs saat ini? Alasannya ?**

Jawaban :

Keuangan, perbendaharaan, akuntansi, asuhan keperawatan,
Alasannya, karena aplikasi- aplikasi keuangan tersebut masih terkendala masalah pelaporan.

Administrator SIMRS EDP

([illegible])

Gambar A.8. Lampiran Wawancara 8

Narasumber : Sawalina, S.Kom
Jabatan : Bagian Software dan Pelaporan
Waktu : 20 Juli 2020
Lokasi : Kantor EDP RSUD Arifin Achmad

Hasil Wawancara

Pertanyaan : **Tanggung jawab di EDP ?**

Jawaban :

Staf edp merangkap analis dan programer.

Pertanyaan : **Apa saja permasalahan/kendala yang sering di jumpai berkaitan dengan TI khususnya SIMRS?**

Jawaban :

- Ada beberapa modul yang belum selesai atau harus disesuaikan lagi dengan kebutuhan RSUD. contohnya stok opname farmasi belum ada, kunjungan pasien di poli, diagnosa penyakit, rawat inap , rawat jalan, radiologi (dokter pemeriksa belum ada di aplikasi), pelaporan farmasi, bagian akuntansi belum berjalan, Permintaan poli masih manual, order obat masih manual.
- Jaringan sering terputus,

Pertanyaan : **Adakah Standar Operasional yang menunjang kinerja dari edp ?**

Jawaban :

Tidak SOP khusus yang mengatur dan memandu edp dalam menangani TI khusunya SIMRS, tidak adanya sharing knowledge antara vendor dan EDP yang mengakibatkan staf edp harus mampu menangani masalah secara mandiri.

Gambar A.9. Lampiran Wawancara 9

Pertanyaan : **Apakah pihak vendor menyediakan manual book atau panduan SIMRS ?**

Jawaban :

Ada namun tidak lagi sesuai dengan perubahan/perkembangan dari SIMRS yang ada pada saat ini.

Pekanbaru, 23 Agustus 2020

(Sawalina, S.Kom)

Gambar A.10. Lampiran Wawancara 10

Narasumber : Ike Emanarni
Jabatan : Administrasi EDP
Waktu :19 Juli 2020
Lokasi :

Hasil Wawancara

Pertanyaan : **Tanggung jawab di EDP ?**

Jawaban :

Jobdesk sebenarnya menangani surat masuk dan surat keluar, namun sekarang merangkap sebagai Administrator SIMRS di edp.

Pertanyaan : **Apa saja permasalahan/kendala yang sering di jumpai berkaitan dengan TI khususnya SIMRS?**

Jawaban :

- Data registrasi redudan akibat permasalahan jaringan.
- Labor dan Radiologi bisa melakukan pendaftaran sendiri sehingga menimbulkan redudansi data apa bila rekomendasi dari irj,ird, maupun irna terlambat.
- Jaringan sering terputus,

Pertanyaan : **Ada tidak pencatatan masalah yang terjadi ?**

Jawaban :

Tidak ada karena masalah yang terjadi sudah kerap kali sehingga dianggap biasa.

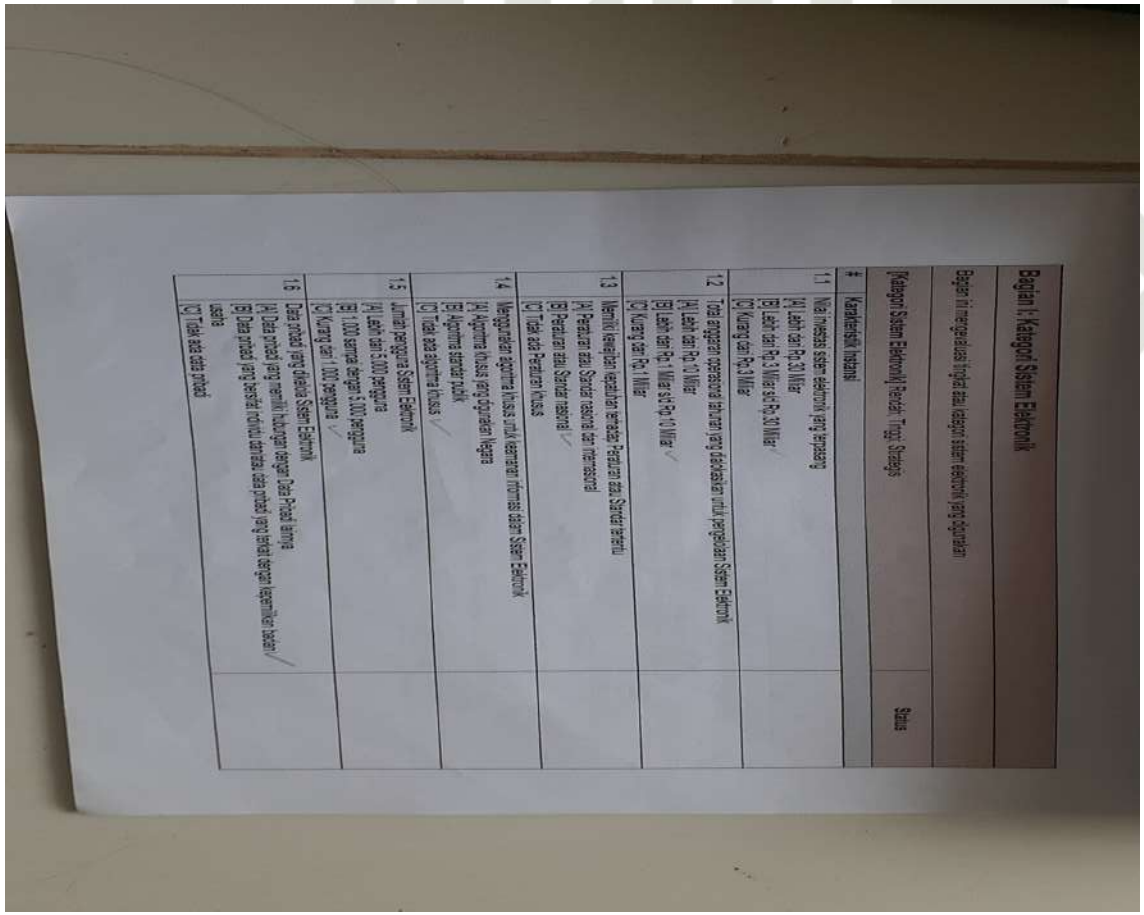
Pekanbaru, 23 Agustus 2020
Administrator SIMRS EDP

(Ike Emanarni)

Gambar A.11. Lampiran Wawancara 11

LAMPIRAN B

HASIL KUISIONER



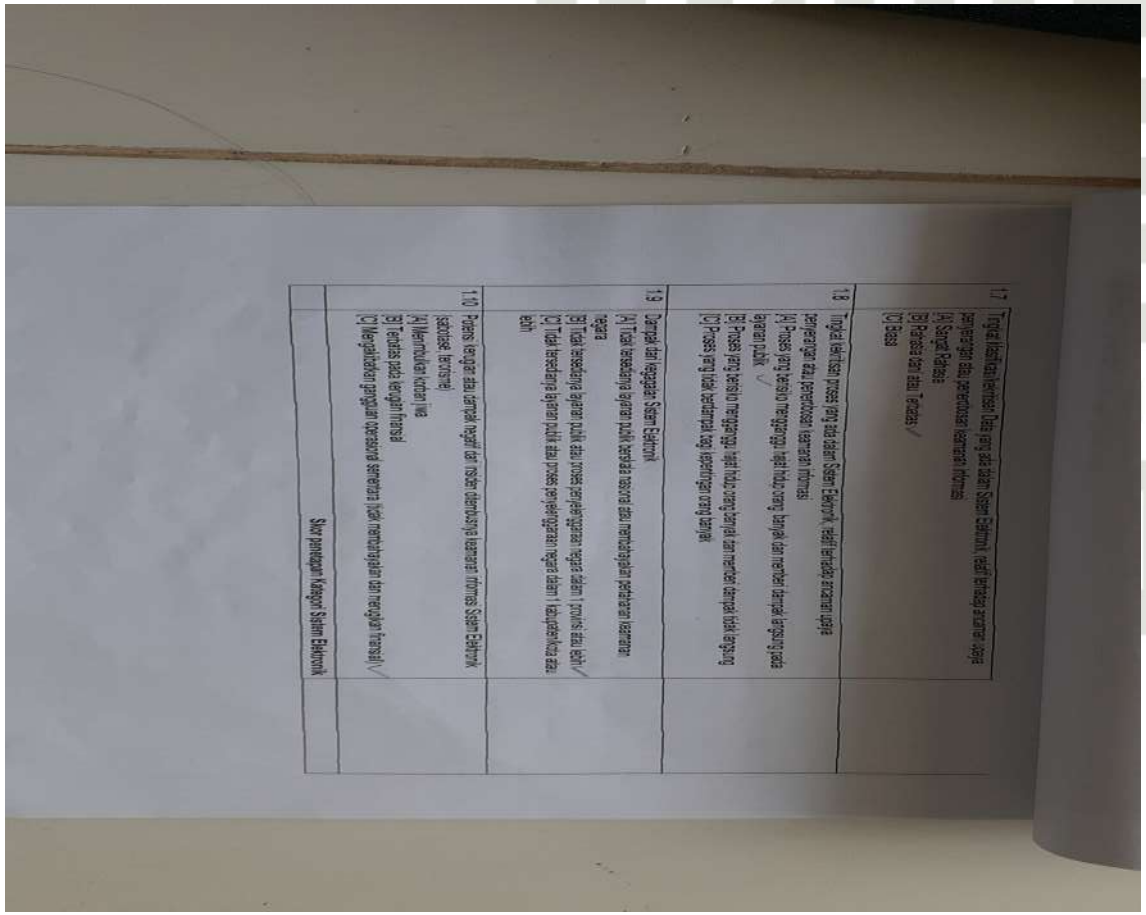
Bagian 1: Kategori Sistem Elektronik

Berapa nilai pengaruh tinggi atau rendah sistem elektronik yang dipunyai

(Kategori Sistem Elektronik) Rendah Tinggi Strategis

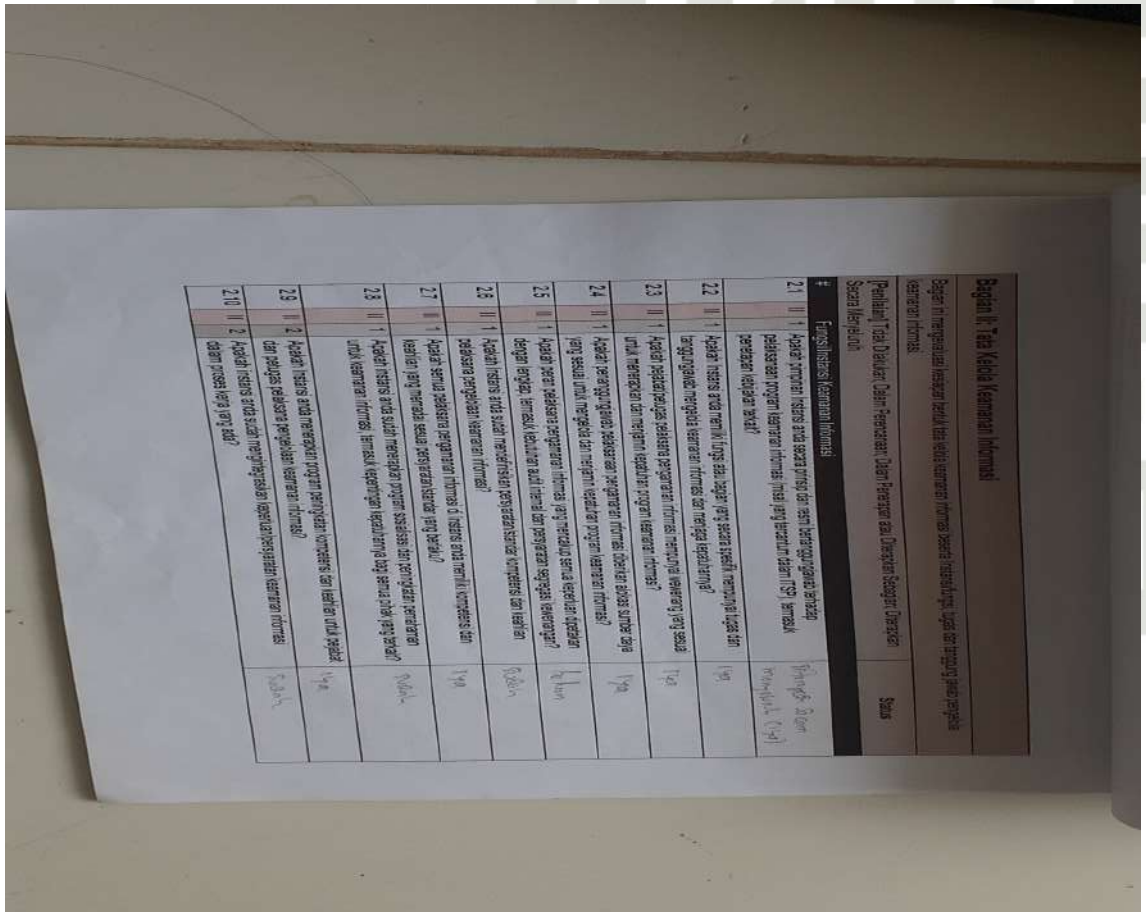
#	Karakteristik Instansi	Status
1.1	Nilai investasi sistem elektronik yang terpasang [A1] Lebih dari Rp.30 Miliar [B1] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C1] Kurang dari Rp.3 Miliar	
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A1] Lebih dari Rp.10 Miliar [B1] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C1] Kurang dari Rp.1 Miliar ✓	
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A1] Peraturan atau Standar nasional dan internasional [B1] Peraturan atau Standar nasional ✓ [C1] Tidak ada Peraturan khusus	
1.4	Menggunakan algoritma khusus untuk kerahasiaan informasi dalam Sistem Elektronik [A1] Algoritma khusus yang dipersyaratkan Negara [B1] Algoritma standar publik [C1] Tidak ada algoritma khusus ✓	
1.5	Jumlah pengguna Sistem Elektronik [A1] Lebih dari 5.000 pengguna [B1] 1.000 sampai dengan 5.000 pengguna [C1] Kurang dari 1.000 pengguna ✓	
1.6	Data pribadi yang dikelola Sistem Elektronik [A1] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B1] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C1] Tidak ada data pribadi ✓	

Gambar B.1. Lampiran Hasil Kuisioner 1

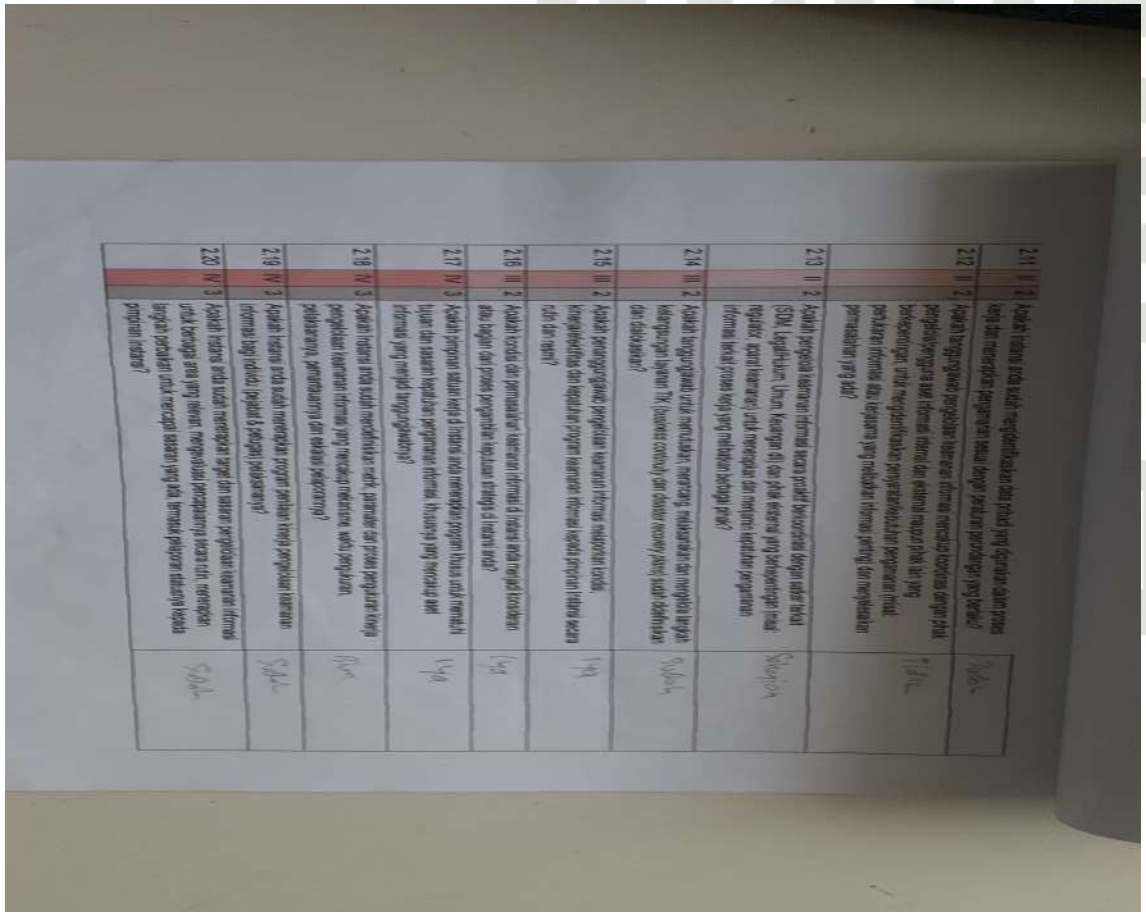


1.7	Tingkat kepentingan Data yang ada dalam Sistem Elektronik, telah terlindungi dengan baik dari pengaksesan, penyebarluasan, dan perubahan oleh pihak yang tidak berwenang	
	[A] Sangat Rahasia	
	[B] Rahasia dan atau Terbatas	
	[C] Biasa	
1.8	Tingkat kepentingan proses yang ada dalam Sistem Elektronik, telah terlindungi dengan baik dari pengaksesan, penyebarluasan, dan perubahan oleh pihak yang tidak berwenang	
	[A] Proses yang sangat mendukung layanan publik yang bersifat rahasia dan membutuhkan tingkat keamanan tinggi pada pelayanan publik	
	[B] Proses yang berkaitan dengan layanan publik dan proses penyelenggaraan negara	
	[C] Proses yang tidak berhubungan dengan layanan publik dan penyelenggaraan negara	
1.9	Dampak dari kegagalan Sistem Elektronik	
	[A] Tidak berkaitan dengan layanan publik, kerahasiaan data, dan membahayakan pertahanan keamanan negara	
	[B] Tidak berkaitan dengan layanan publik atau proses penyelenggaraan negara dalam provinsi atau lebih	
	[C] Tidak berkaitan dengan layanan publik atau proses penyelenggaraan negara dalam Kabupaten/Kota atau lebih	
1.10	Potensi kerugian atau dampak negatif dari insiden dalam ruang lingkup keamanan informasi Sistem Elektronik (sabotase, terorisme)	
	[A] Menimbulkan korban jiwa	
	[B] Berdampak pada kerugian finansial	
	[C] Mengganggu pelayanan operasional sementara tidak membahayakan kerugian finansial	
	Skor penilaian Kategori Sistem Elektronik	

Gambar B.2. Lampiran Hasil kuisioner 3



Gambar B.3. Lampiran Hasil kuisioner 4

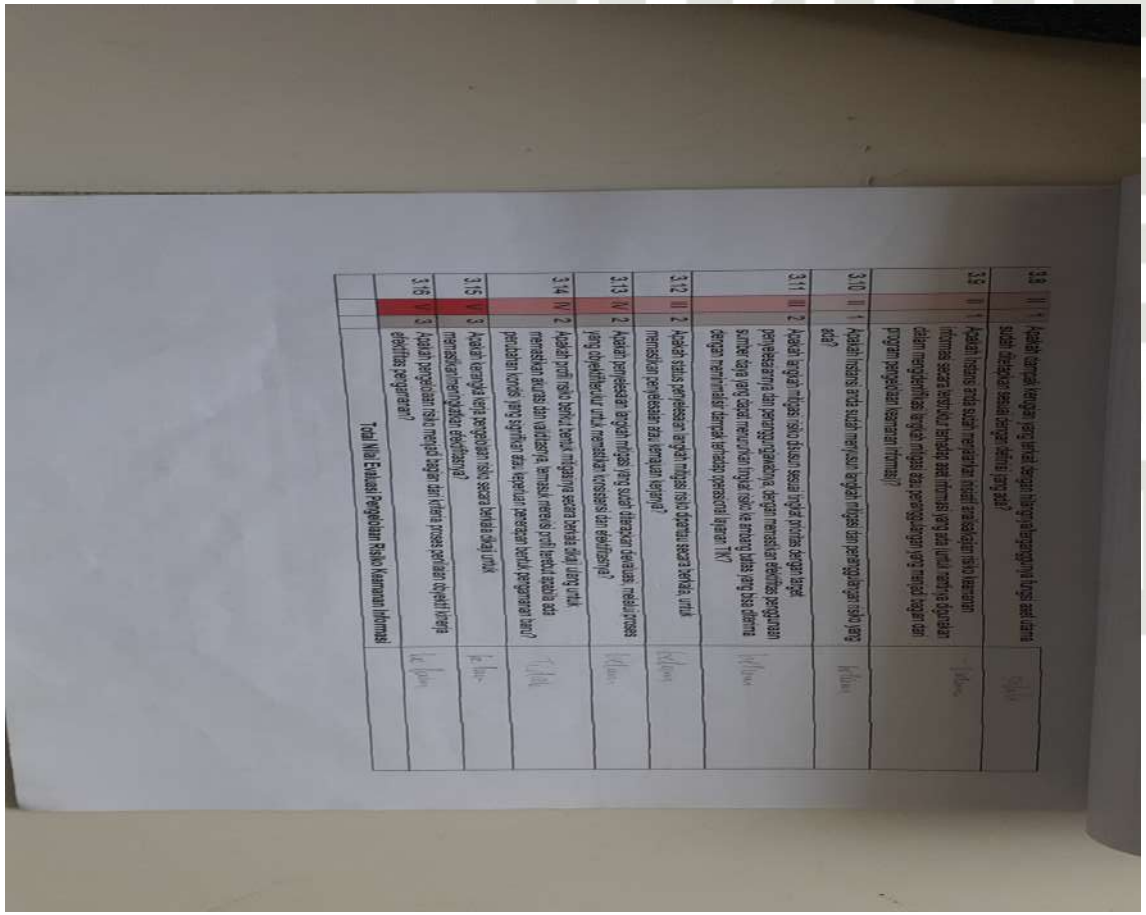


Gambar B.4. Lampiran Hasil kuisioner 5

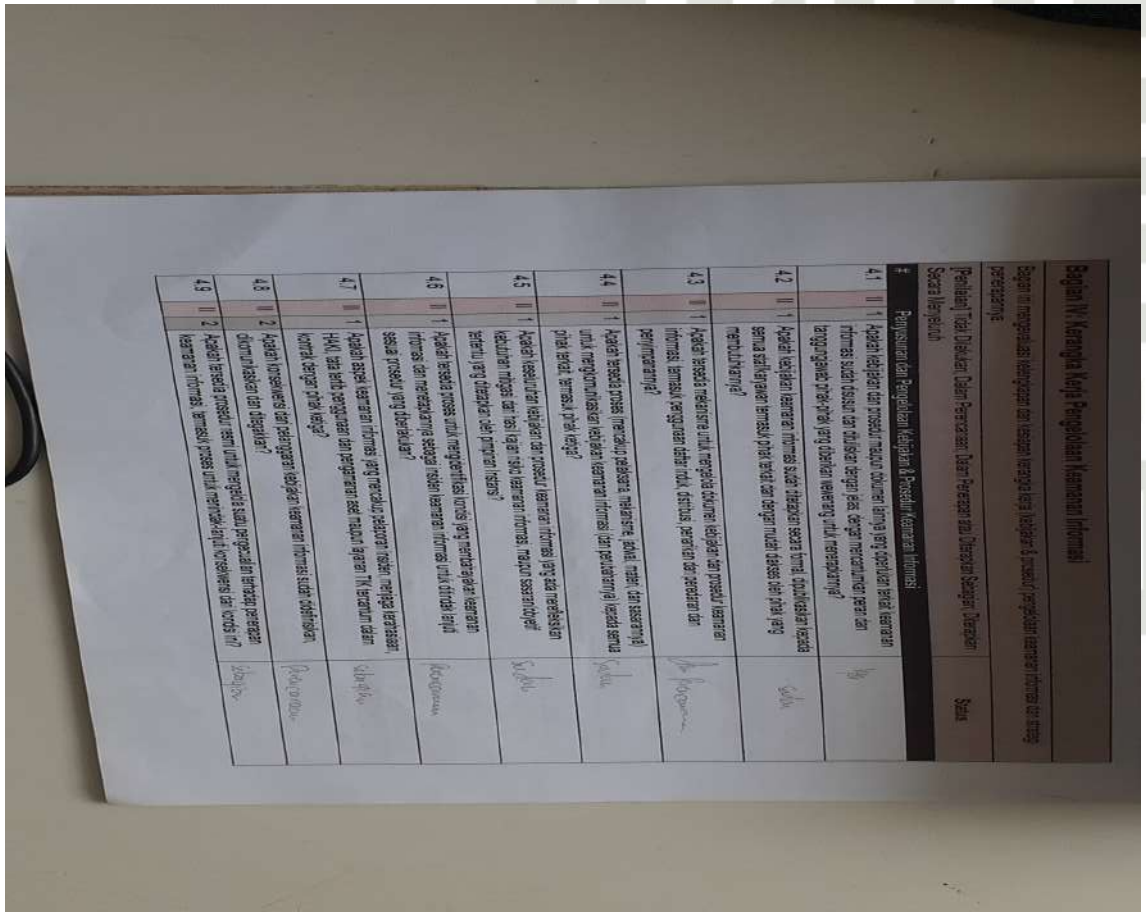
2.2.1	IV	3	Apakah instansi anda sudah mengidentifikasi kejadian, penyakit hukum dan bahaya lainnya tentang keamanan informasi yang harus dipatuhi dan mengevaluasi tingkat kepatuhannya?	
2.2.2	IV	3	Apakah instansi anda sudah mendokumentasikan kejadian dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	
			Total Nilai Evaluasi Tata Kelola	

Bagian III: Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi kesiapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.	
[Penilaian] Tidak Dilakukan Dalam Penerapan, Dalam Penerapan atau Diterapkan Secara Menyeluruh	Status
Kajian Risiko Keamanan Informasi	
3.1.1 Apakah instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	
3.2.1 Apakah instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	
3.3.1 Apakah instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	
3.4.1 Apakah kerangka kerja pengelolaan risiko tersebut mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi anda?	
3.5.1 Apakah instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	
3.6.1 Apakah instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	
3.7.1 Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	

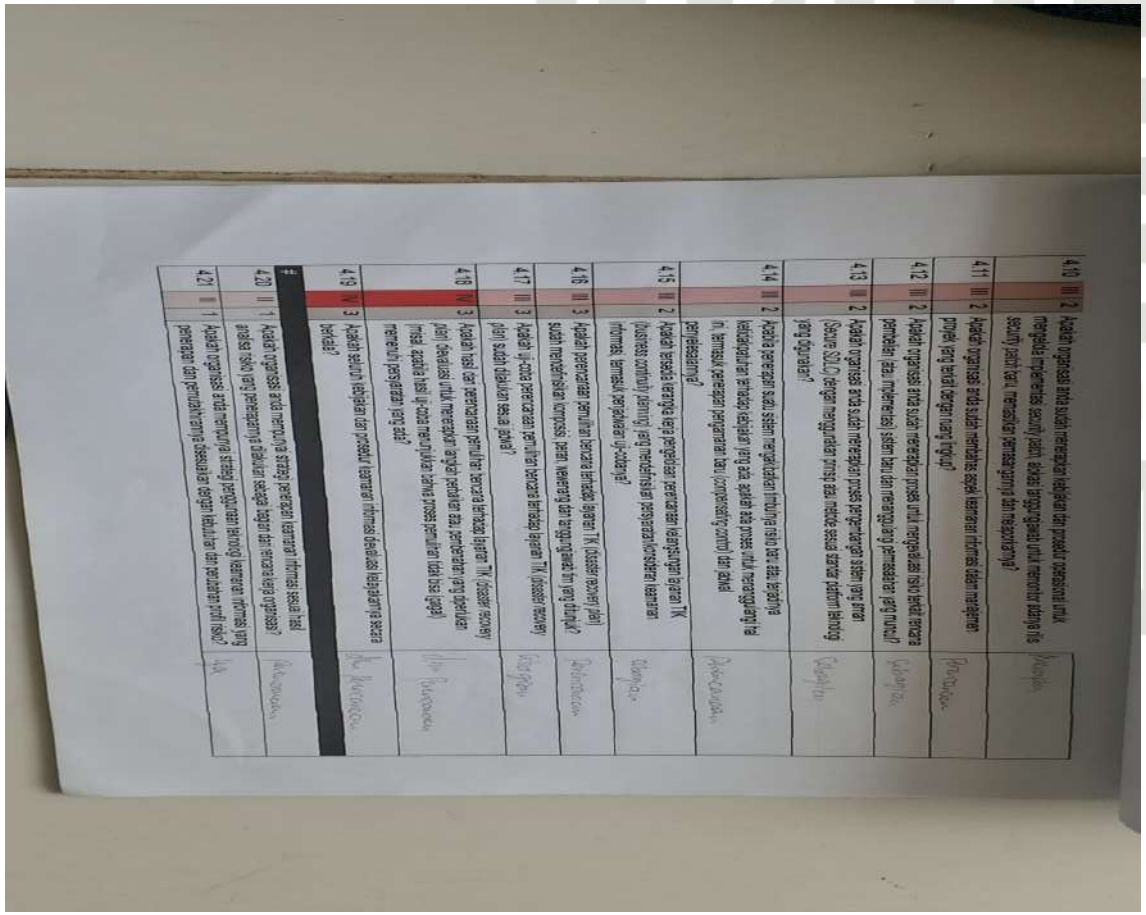


Gambar B.6. Lampiran Hasil kuisioner 7

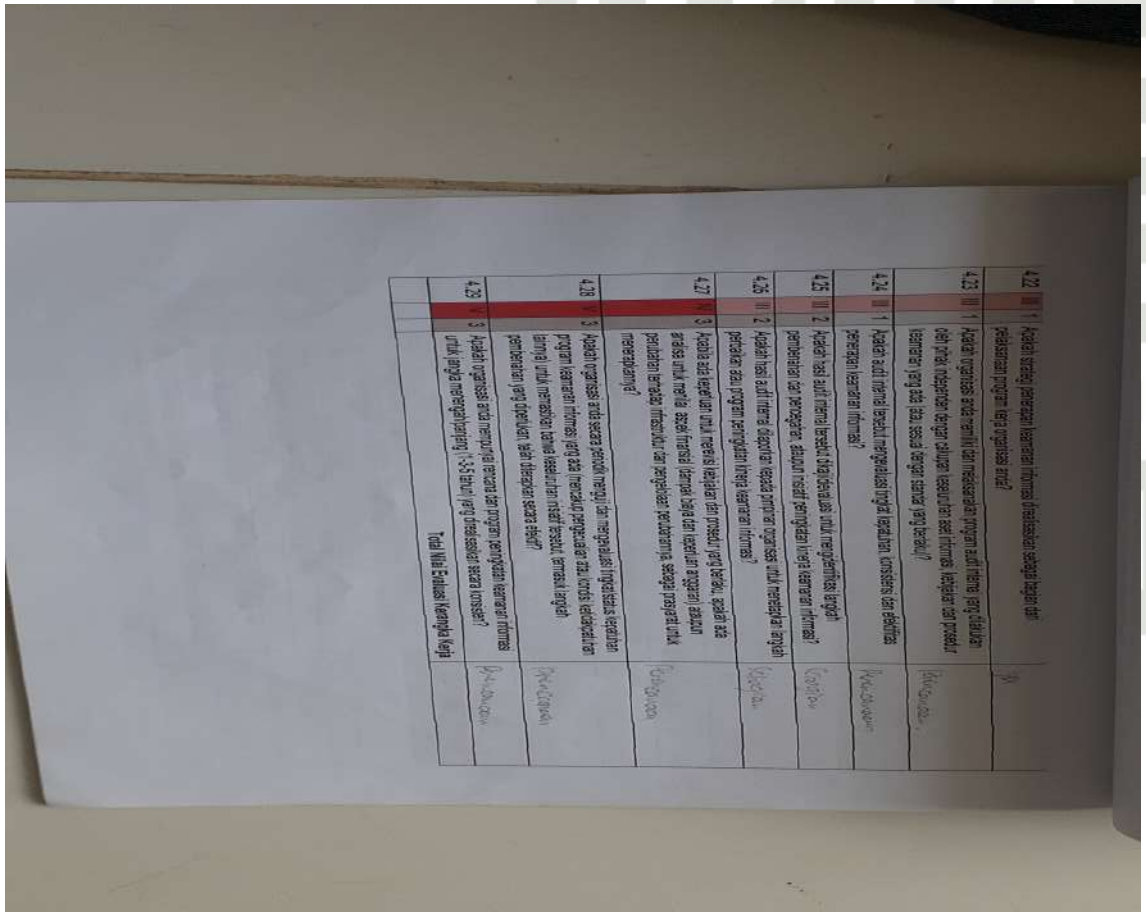


Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi		
Bagian ini mengevaluasi kelengkapan dan kesesuaian kerangka kerja pengelolaan keamanan informasi di unit yang dinilai		
[Penilaian] Telah Dilakukan Dalam Penerapan Aspek Pengelolaan Keamanan Informasi Secara Menyeluruh	Status	
#	Pertanyaan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi	
4.1	III 1 Apakah kebijakan dan prosedur operasional untuk pengelolaan teknologi informasi sudah didokumentasikan dan dikomunikasikan dengan baik kepada pihak-pihak yang membutuhkannya?	Ya
	II 2 Bagaimana proses pengkajian dan pembaruan kebijakan dan prosedur operasional dilakukan?	
4.2	III 1 Apakah terdapat kebijakan khusus untuk pengamanan informasi pada pihak ketiga (seperti vendor dan pelanggan) serta mekanisme untuk mengendalikan risiko yang terkait dengan akses pihak ketiga tersebut?	Sudah
	II 2 Bagaimana proses identifikasi risiko pihak ketiga dan penerapan pengamanan yang sesuai dilakukan?	
4.3	III 1 Apakah terdapat mekanisme untuk mengelola dokumen kebijakan dan prosedur operasional, termasuk pengendalian versi dan distribusinya?	Sudah
	II 2 Bagaimana proses pengendalian perubahan dokumen dilakukan untuk memastikan hanya versi terbaru yang digunakan?	
4.4	III 1 Apakah terdapat proses manajemen perubahan terhadap infrastruktur teknologi informasi dan sistem informasi untuk meminimalkan risiko gangguan operasional?	Sudah
	II 2 Bagaimana proses tersebut memastikan perubahan telah diuji dan disetujui sebelum diterapkan?	
4.5	III 1 Apakah terdapat prosedur pengelolaan insiden keamanan informasi yang mencakup pelaporan, penanganan, dan pemulihan?	Sudah
	II 2 Bagaimana prosedur tersebut memastikan insiden ditangani dengan cepat dan efektif?	
4.6	III 1 Apakah terdapat proses untuk mengidentifikasi aset informasi yang kritis dan menentukan pemiliknya?	Sudah
	II 2 Bagaimana proses identifikasi dan klasifikasi aset informasi dilakukan, dan bagaimana pemilik aset ditentukan?	
4.7	III 1 Apakah terdapat prosedur yang mengatur penggunaan aset TI, termasuk penggunaan HAKI dan aset pihak ketiga?	Sudah
	II 2 Bagaimana prosedur tersebut memastikan penggunaan aset sesuai dengan kebijakan yang berlaku?	
4.8	II 2 Apakah terdapat kebijakan khusus yang mengatur penggunaan perangkat milik pribadi untuk keperluan pekerjaan?	Sudah
4.9	II 2 Apakah terdapat prosedur untuk mengelola data pribadi yang diproses melalui perangkat tersebut?	Sudah

Gambar B.7. Lampiran Hasil kuisioner 8



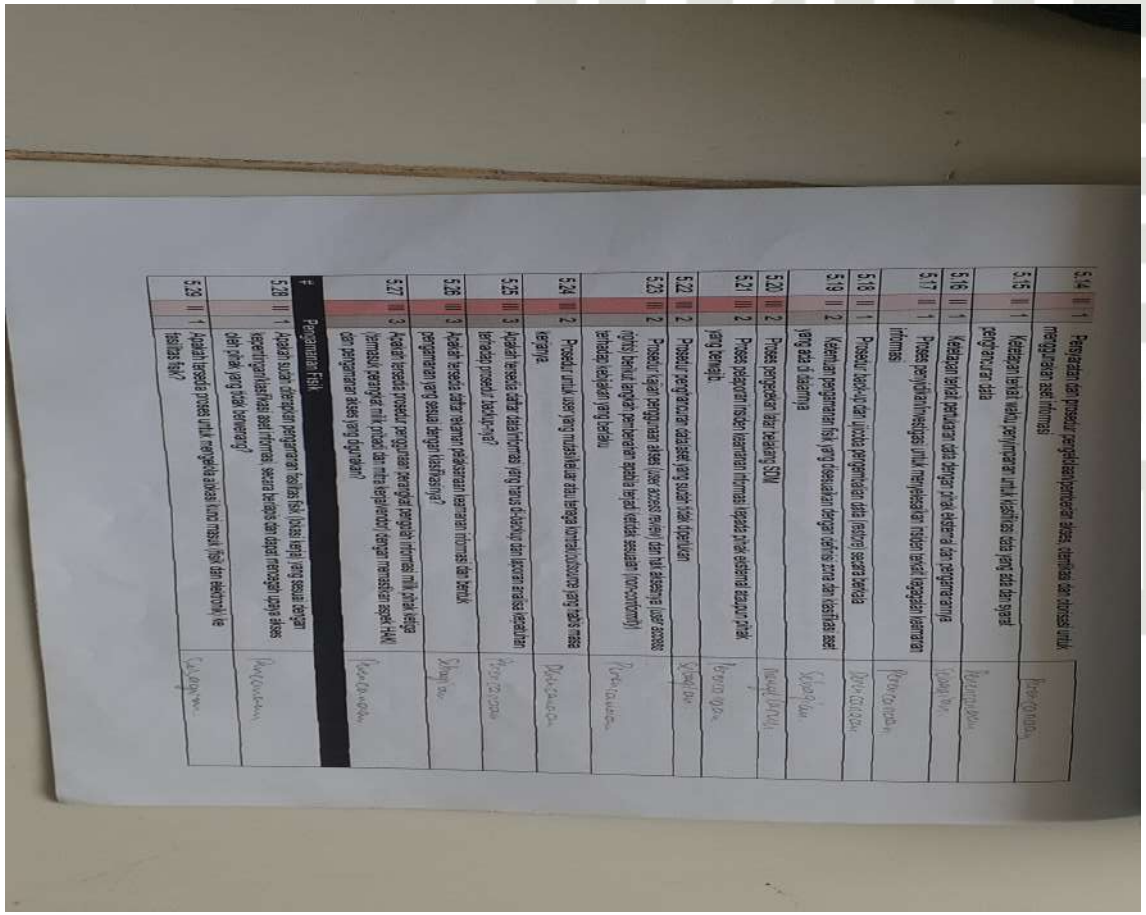
Gambar B.8. Lampiran Hasil kuisioner 9



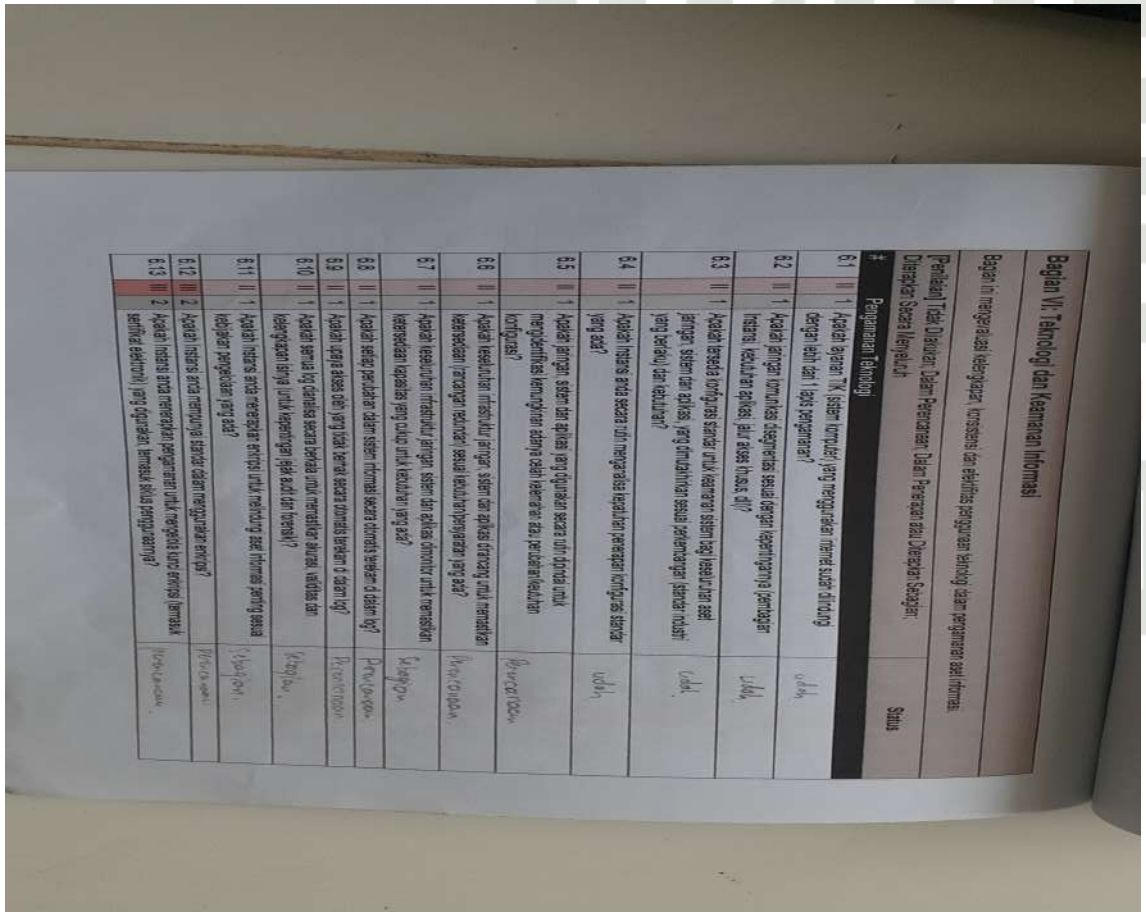
Gambar B.9. Lampiran Hasil kuisioner 10

Bagian V: Pengelolaan Aset Informasi				
Bagian ini mengevaluasi kepatuhan pengelolaan aset informasi, termasuk kesesuaian akses pengguna aset tersebut.				
[Pemilihan] Tidak Dilakukan Dalam Pemrosesan Dalam Penerapan atau Diterapkan Sebagian Diterapkan Secara Menyeluruh				Status
#	Pengelolaan Aset Informasi			
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpercaya? (termasuk kepemilikan aset.)	II	↑	ada
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	II	↑	ada
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan kepatuhan pengamanannya?	II	↑	Iyah ditemui
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dan siapa saja yang berhak dan matrix yang merekam akses akses tersebut	II	↑	Ditemukan
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang dirangkum secara komperhensif?	II	↑	Sudah ada
5.6	Apakah tersedia proses pengelolaan konfigurasi yang dirangkum secara komperhensif?	II	↑	Ada
5.7	Apakah tersedia proses untuk mendisposisi aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	II	↑	Sudah ada
	Apakah instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dan proses pemrosesan milyaki nisc?			
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil instansi anda	II	↑	Ada
5.9	Tata tertib penggunaan komputer, email, internet dan intranet	II	↑	Ada
5.10	Tata tertib pengamanan dan penggunaan aset instansi terkait HAKI	II	↑	Ada
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	II	↑	Ada
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	II	↑	Belum ada
5.13	Pengelolaan identitas elektronik dan proses autentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	II	↑	Sudah ada

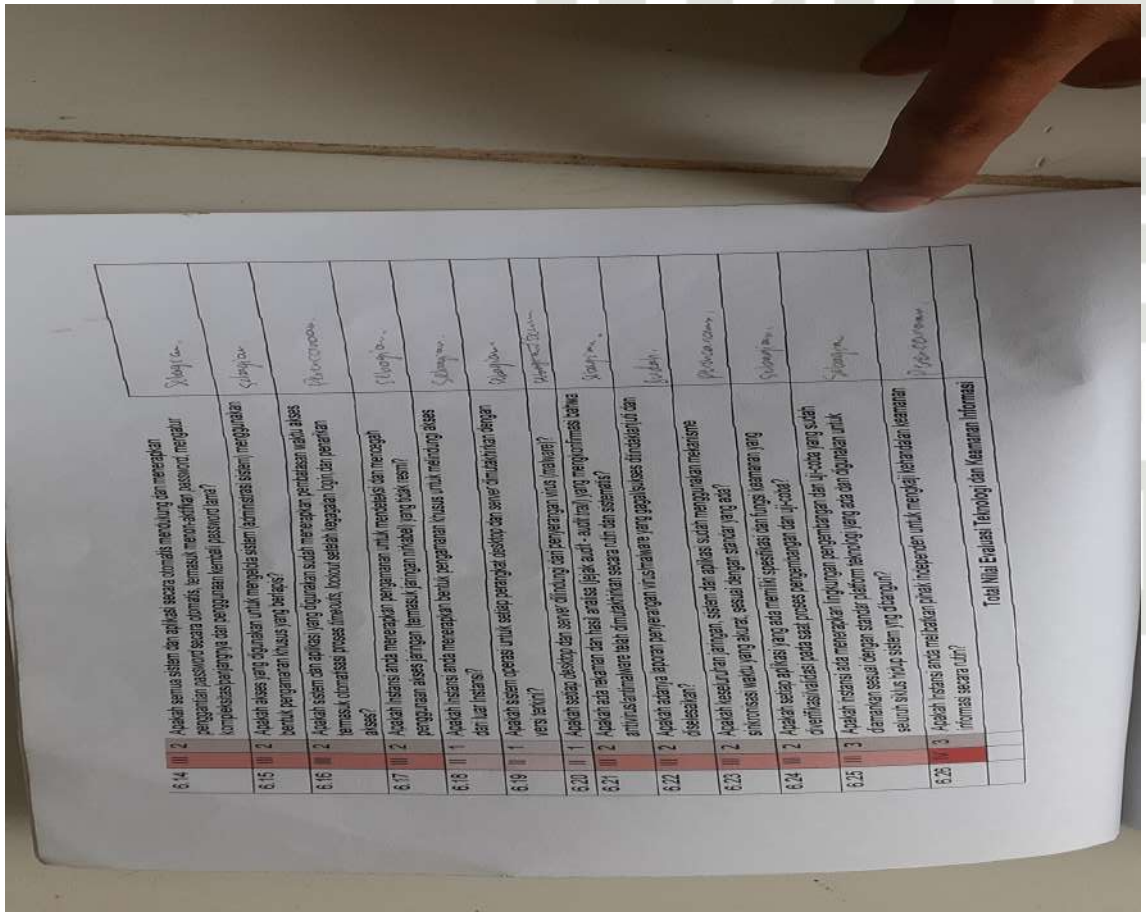
Gambar B.10. Lampiran Hasil kuisioner 11



Gambar B.11. Lampiran Hasil kuisioner 12



Gambar B.12. Lampiran Hasil kuisioner 13



6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?		
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrator sistem) menggunakan bentuk pengamanan khusus yang berlapis?		
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login dan penarikan akses?		
6.17	III	2	Apakah instansi anda menerapkan pengamanan untuk mencegah dan mendeteksi dan server dimanfaatkan dengan pengunaan akses jaringan termasuk jaringan nirkabel) yang tidak resmi?		
6.18	II	1	Apakah instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi?		
6.19	II	1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?		
6.20	II	1	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?		
6.21	III	2	Apakah ada laporan dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?		
6.22	II	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?		
6.23	III	2	Apakah keseluruhan jaringan sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?		
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?		
6.25	III	3	Apakah instansi anda menerapkan lingkungan pengembangan dan uji-coba yang sudah diterapkan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?		
6.26	IV	3	Apakah instansi anda melakukan pihak independen untuk mengaji kelayakan keamanan informasi secara rutin?		
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi		

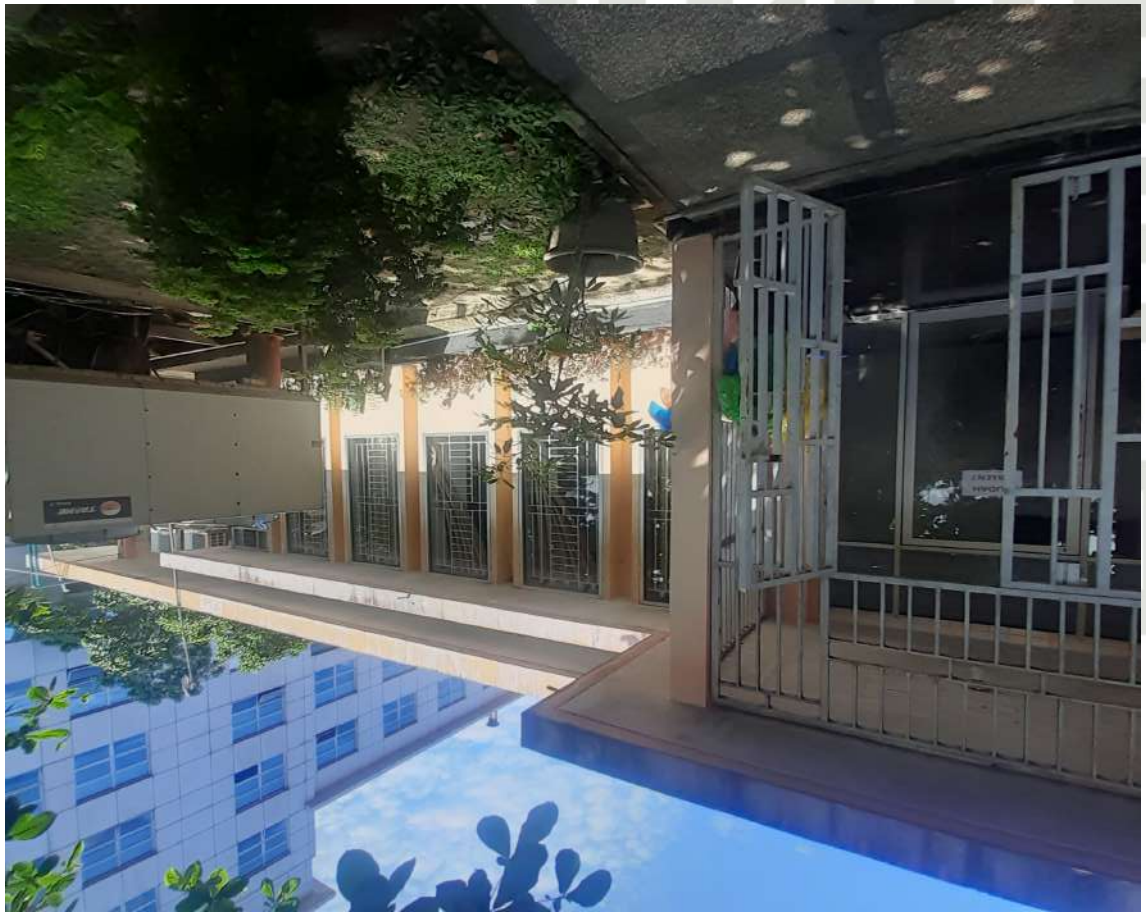
Gambar B.13. Lampiran Hasil kuisioner 14

LAMPIRAN C
DOKUMENTASI

Gambar C.1. Lampiran Dokumentasi 1

Gambar C.2. Lampiran Dokumentasi 2

Gambar C.3. Lampiran Dokumentasi 3



Gambar C.4. Lampiran Dokumentasi 4

Gambar C.5. Lampiran Dokumentasi 5

DAFTAR RIWAYAT HIDUP

Penulis dilahirkan di Payakumbuh, Kecamatan Payakumbuh Barat, Kabupaten 50 Kota, Provinsi Sumatra Barat pada tanggal 03 Oktober 1996, yang diberi nama Mohamat Iqbal. Penulis merupakan anak ke dua dari tiga bersaudara. Putra dari pasanganan Bapak Yohanson dan Ibu Yuni Rika. Penulis beralamat di Payakumbuh,kabupaten lima puluh kota.

Pada tahun 2003 penulis pertama kali menempuh pendidikan di SDN 028 Titian Antui,Duri dan selesai pada tahun 2009. Selanjutnya penulis melanjutkan pendidikan di SMP Negeri 2 mandau dan selesai pada tahun tahun 2012. Pada tahun 2012 penulis melanjutkan pendidikan di SMAN 1 Mandau dan selesai pada tahun 2015. Pada tahun 2015 penulis melanjutkan pendidikan ke perguruan tinggi yakni di Universitas Islam Negeri Sultan Syarif Kasim Riau melalui jalur SBMPTN dan diterima sebagai mahasiswa jurusan Sistem Informasi Fakultas Sains dan Teknologi.

Pada tahun 2017 semasa kuliah penulis melaksanakan Kerja Praktek (KP) pada UPTD Hortikultura dan pangan Pekanbaru. Penulis juga ikut serta dalam Kuliah Kerja Nyata (KKN) yang bertempat di desa Sungai Ambang, Kecamatan Rumbai Pesisir, Kota Pekanbaru. Dengan demikian, penulis mengucapkan rasa syukur atas selesainya Laporan Tugas Akhir ini yang berjudul "Evaluasi Keamanan Sistem Informasi RSUD Arifin Achmad Menggunakan ISO 27001". Untuk menjalin silahturahmi berikut kontak person penulis yang dapat dihubungi No. Hp: +6282287417655 dan juga dapat melalui E-mail: mohamat.iqbal@students.uin-suska.ac.id.